Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Nom du projet	**sedex**
Numéro de projet	5664
Document	**Manuel sedex**
Version	**4.0.4 (06.09.2013)**

	en travail	en examen	autorisé pour l'utilisation
Statut	☐	☐	X

Données dans WORD:	
Titre	**Manuel sedex**
Date d'enregistrement	06.09.2013 09:35:00
Nom du fichier	sedex_v4_0_4_hb_fr
Emplacement	
Auteur(s)	OFS
Commentaires	

Compétences (la diffusion dépend du statut coché ci-dessus):

Auteurs/Conception:	Rollout sedex
Examen/Approbation:	Stefan Podolak
Utilisateurs:	Fournisseurs de logiciel
Pour information:	

Suivi des modifications

Version	*Date*	*Nom ou rôle*	*Remarque*
3.0	28.11.2008	Ralph Köchli	Révision totale suite à la séparation du manuel
3.1	08.07.2009	Ralph Köchli	Diverses modifications selon les release-notes
3.2	09.12.2009	Michel Gentile	Diverses modifications selon les release-notes
3.3	24.06.2010	Michel Gentile	Diverses modifications selon les release-notes
4.0	14.04.2011	Michel Gentile	Diverses modifications selon les release-notes
4.0.1	25.08.2011	Michel Gentile	Diverses modifications selon les release-notes
4.0.3	15.11.2012	Michel Gentile	Diverses modifications selon les release-notes
4.0.4	06.09.2013	Michel Gentile	Modifications aux chapitres 1, 2.2.1, 2.3, 3.10, 4.4.3.1, 4.7.1, 8.1

Approbation

Version	*Date*	*Nom ou rôle*	*Remarque*
3.0	28.11.2008	Nedim Muratbegovic	
3.1	08.07.2009	Nedim Muratbegovic	
3.2	09.12.2009	Nedim Muratbegovic	
3.3	24.06.2010	Nedim Muratbegovic	
4.0	14.04.2011	Nedim Muratbegovic	
4.0.1	25.08.2011	Nedim Muratbegovic	
4.0.3	15.11.2012	Nedim Muratbegovic	
4.0.4	06.09.2013	Stefan Podolak	

Table des matières

1	**Introduction**	**6**
1.1	Définition de sedex	6
1.2	Objectif du document	6
1.3	Version du document	6
1.4	Références	7
1.5	Glossaire	8
2	**Architecture sedex**	**10**
2.1	Introduction	10
2.2	Composants de l'architecture	11
2.2.1	Vue d'ensemble	11
2.2.2	Le serveur sedex	11
2.2.3	Liste des participants	11
2.2.4	L'adaptateur sedex	12
2.2.5	Proxy service web	12
2.2.6	Controller	13
2.2.7	Client	13
2.3	Scénarios de communication	14
2.4	Possibilités de raccordement à sedex	16
2.4.1	Raccordement physique	16
2.4.2	Raccordement logique	17
2.4.3	Indépendance à l'égard de l'adressage des messages	18
3	**Utilisation de sedex**	**19**
3.1	Structure de répertoire du client sedex	19
3.1.1	Client sedex < V4.0	19
3.1.2	Client sedex ≥ V4.0	21
3.2	Interface entre l'application et l'adaptateur	23
3.2.1	Répertoires d'interface	24
3.3	Echange de messages	25
3.3.1	Envoi d'un message sedex	25
3.3.2	Réception d'un message sedex	26
3.4	Convention d'écriture	27
3.5	Mise à disposition de messages	27
3.6	Contenu de l'enveloppe	28
3.7	Contenu de la quittance	32
3.8	Adressage	34
3.8.1	Vue d'ensemble	34
3.8.2	Niveaux institutionnels et unités organisationnelles	34
3.8.3	Code de fonction	35
3.8.4	Exemples	37
3.9	Catégories d'erreurs et codes de statut	37
3.9.1	Catégories d'erreurs	37
3.9.2	Codes de statut	38
3.9.3	Comportement en cas d'enveloppe incorrecte (statut 200)	42
3.9.4	Gestion des doublons en matière de message ID (statut 201)	42
3.9.5	Comportement lors d'erreurs de réseau	43
3.9.6	Calcul de la date de péremption d'un message (codes de statut 203, 204 et 701)	43
3.10	Exemples	44
3.10.1	Exemple: livraison de la commune d'Olten à la statistique	44

3.11	Proxy service web	47
3.11.1	But du Proxy service web	47
3.11.2	Fonctionnement du Proxy service web	47
3.11.3	Echange de messages	47
3.11.4	Accès au Proxy service web	48
3.11.5	Services web compatibles	48
3.12	Aspects de l'exploitation de l'adaptateur sedex	48
3.12.1	Délais de conservation	48
3.12.2	Version du schéma XML eCH-0090	48
3.13	Messages de service sedex	49
3.14	Polling	49
3.15	Surveillance des composants	50
3.15.1	Fichier monitoring	51
3.15.2	Requête HTTP	51
3.16	Optimisation du client sedex	52
3.17	Verrouillage des applications	52
3.18	Assistance à distance	53
3.18.1	Mécanisme des commandes	53
3.18.2	Récupération de la configuration et des logs	53
3.18.3	Mise à jour	53
3.19	Journalisation	53
4	**Processus**	**54**
4.1	Vue d'ensemble	54
4.2	Certification des applications participantes	54
4.3	Annonce d'un participant	54
4.3.1	Préparer l'annonce	54
4.3.2	Annoncer les participants à l'OFS	55
4.4	Installation du client sedex	55
4.4.1	Exigences en matière de configuration réseau	55
4.4.2	Préparation de la configuration réseau	56
4.4.3	Installation	60
4.5	Modification des autorisations / routage	61
4.5.1	Modification des autorisations	61
4.5.2	Modification du routage	61
4.6	Renouvellement du certificat d'organisation	61
4.6.1	Types de renouvellement	61
4.6.2	Renouvellement automatique	61
4.6.3	Renouvellement manuel	62
4.7	Management des mises à jour	62
4.7.1	Support des différentes versions	63
4.8	Exploitation	63
4.9	Frequently Asked Questions (FAQ)	63
5	**Compétences**	**64**
5.1	Service clientèle de l'OFS	64
5.1.1	Prestations	64
5.1.2	Contact	64
5.2	Fournisseur	64
5.3	Participants	64
5.4	Coordination avec un domaine technique	65
5.4.1	Tâches	65
5.4.2	Coordinateurs actuels des domaines techniques	65
6	**Test et intégration**	**66**

6.1	Types de tests	66
6.1.1	Tests sedex	66
6.1.2	Tests End-to-End	66
6.2	Instances de tests	66
6.3	Messages de tests	67
6.4	Intégration	67
7	**Sécurité**	**68**
7.1	Principes de base des réflexions concernant la sécurité	68
7.2	Vue d'ensemble du système sedex	68
7.3	Attente à l'égard des applications participantes	69
7.4	Evaluation des risques de sécurité pour l'émetteur et le récepteur	69
7.5	Composants de la sécurité - certificats de sécurité	70
7.6	Renouvellement des certificats de sécurité	70
7.6.1	La problématique de la mise à jour des certificats de sécurité	70
8	**Annexe**	**72**
8.1	Schémas XML	72
8.2	Règles pour les documents XML	72
8.2.1	Codage des documents XML	72
8.2.2	Indications de temps	72
8.3	Service web CheckSedex	72
8.3.1	Description du service	72
8.3.2	Limitations	73
8.3.3	Configuration requise	73
8.3.4	Paramètres d'envoi	73
8.3.5	Paramètres de réponse	74
8.4	Processus standard pour la distribution de certificats d'organisation	75
8.4.1	Première distribution et renouvellement manuel	75
8.4.2	Renouvellement automatique	76
8.4.3	Inconvénients du renouvellement manuel du certificat	76
8.4.4	Procédure pour retrouver la date d'expiration du certificat d'organisation	77
8.5	Fichier logs	81
8.5.1	Contexte	81
8.5.2	Description des fichiers	81
8.5.3	Logs du controller	82
8.5.4	Logs de l'adaptateur	82
8.5.5	Logs du proxy service web	85
8.5.6	Configuration	86
8.5.7	Annexes	86

1 Introduction

1.1 Définition de sedex

Dans le cadre de l'harmonisation des registres fédéraux de personnes et des registres cantonaux et communaux de l'habitant, la Confédération propose depuis 2008 une plateforme pour l'échange sécurisé de données.

Cette plateforme, baptisée sedex (secure date exchange), permet aux participants d'échanger des données de manière sécurisée. A la différence des systèmes de mailing habituels, ce système, qui communique de manière asynchrone, permet d'échanger simultanément un très grand nombre de messages.

sedex peut être utilisé dans d'autres domaines, même s'il est réservé en priorité aux applications entrant dans le cadre de l'e-Government.

Pour raccorder une application participante à sedex, il faut y intégrer un adaptateur sedex et remplir les exigences fixées en matière de sécurité (authentification et certification).

A partir de la version 2.0, l'adaptateur sedex inclut un proxy service web permettant une authentification par certificat du participant vis-à-vis d'autres services web, qui n'ont dès lors plus à s'occuper de la gestion des utilisateurs.

La version 4.0 intègre la notion de controller. Ce nouveau composant doit garantir la bonne marche de l'adaptateur sedex et du proxy service web sedex. Ces trois composants sont désormais regroupés sous le nom de client sedex.

1.2 Objectif du document

Ce document décrit le système sedex du point de vue des applications participant à l'interconnexion avec sedex. Il est destiné en premier lieu aux fournisseurs de logiciel développant ce genre d'applications.

Les publics cible de ce document sont:

- les architectes de logiciel
- les développeurs de logiciel
- les responsables de la sécurité
- les exploitants du client sedex

Ce manuel fixe les conditions de mise en œuvre pour les fournisseurs de logiciel qui souhaitent raccorder leur application à sedex ou passer par sedex pour traiter des business use cases. L'Office fédéral de la statistique a établi ce manuel à l'issue de longs travaux d'analyse et au terme de larges consultations. Des adaptations et des modifications ne peuvent cependant pas être exclues.

1.3 Version du document

Chaque version du client sedex fait l'objet d'une version correspondante du manuel sedex. La présente version 4.0.4 fait référence au client sedex V4.0.4 publié le 25 juillet 2013.

1.4 Références

[1] OSCI-Transport 1.2, Spezifikation, OSCI Leitstelle, Bremen, 6.6.2002
http://www1.osci.de/sixcms/media.php/13/osci_spezifikation_1_2_deutsch.pdf

[2] OSCI-Transport 1.2, Entwurfsprinzipien, Sicherheitsziele und -mechanismen, OSCI Leitstelle, Bremen, 6.6.2002
http://www1.osci.de/sixcms/media.php/13/osci_entwurfsprinzipien_1_2.2110.pdf

[3] Office fédéral de la statistique:
Liste historisée des communes de la Suisse – Explications et utilisation (15.06.2007)
http://www.bfs.admin.ch/bfs/portal/fr/index/news/publikationen.html?publicationID=2755

[4] Office fédéral de la statistique:
Manuel sedex - Harmonisation des registres. V 3.1 (08.07.2009)
http://www.registre-stat.admin.ch > Spécifications informatiques > Harmonisation des registres et Service de validation

[5] Office fédéral de la statistique:
Annonces des registres fédéraux aux registres des habitants. V 1.4 (25.08.2011)
http://www.registre-stat.admin.ch > Spécifications informatiques > Echanges entre registres

[6] Centrale de compensation:
UPI (Unique Personal Identifier) Interface. V 1.6 (02.12.2012)
http://www.zas.admin.ch/org/00721/00758/00908/index.html?lang=fr

[7] Office fédéral de l'informatique et de la télécommunication:
sedex Client Installation and User Manual V 4.0.4 (25.07.2013)
http://www.sedex.ch > Clients sedex et documentation

[8] Office fédéral de l'informatique et de la télécommunication:
sedex: Manuel d'utilisation du proxy service web V 3.0.4 (25.07.2013)
http://www.sedex.ch > Clients sedex et documentation

[9] Office fédéral de la statistique:
Types de messages sedex fédéraux et cantonaux, V 3.0.1 (25.07.2013)
http://www.sedex.ch > Clients sedex et documentation

[10] Office fédéral de l'informatique et de la télécommunication:
Handbuch für EBS-Teilbus-Betreiber, V 0.5 (15.12.2010)

[11] Office fédéral de la statistique:
Release-Notes – client sedex V 4.0.4 (25.07.2013)
http://www.sedex.ch > Clients sedex et documentation

1.5 Glossaire

Notion	Signification
Adaptateur	«Elément de liaison» entre les applications participant à l'interconnexion sedex et le système sedex.
Application	Logiciel (système d'un registre) participant à l'interconnexion sedex.
Cardinalité	En parlant d'un fichier de log précis, désigne le nombre d'enregistrement qui doivent être écrits dans ce fichier.
Client	Le client sedex désigne l'installation dans son ensemble comprenant le controller sedex, l'adaptateur sedex et le proxy service web sedex.
ClientDir	Désigne le dossier d'installation du client sedex.
Composant	Désigne un élément du client, qui peut être le controller sedex, l'adaptateur sedex ou le proxy service web sedex.
Controller	Le controller sedex est chargé de garantir la bonne marche de l'adaptateur et du proxy service web en redémarrant, le cas échéant, les composants.
Fournisseur	Fournisseur de logiciel, respectivement son représentant pour l'installation (partenaire de distribution).
HPSA	Adaptateur sedex haute performance (Adaptateur sedex 3.0)
Participant ID	Identification explicite utilisée pour l'adressage des *participants* dans l'interconnexion sedex. Synonyme de *sedex ID*.
sedex ID	Synonyme pour Participant ID
KOMBV/KTV	Réseau de communication reliant les administrations fédérales et cantonales.
Liste des participants	Liste technique dans laquelle sont répertoriés les participants atteignables via sedex
Liste des services administratifs	Liste des services administratifs qui peuvent être atteints via sedex. La liste des services administratifs est provisoirement gérée par l'OFS.
Log	Fichier contenant les événements journalisés par le client sedex.
OFS	Office fédéral de la statistique
Participant	Un système logiciel (par ex. le système d'un service administratif) qui est atteignable via l'interconnexion sedex.
Participant actif	Un *participant* qui peut envoyer et recevoir des messages.
Participant inactif	Un *participant* qui ne peut ni envoyer, ni recevoir des messages
Participant logique	*Participant* mentionné dans la *liste des participants* à sedex mais qui ne dispose ni d'un adaptateur ni d'un certificat indivi-

Notion	Signification
	duel. Un *participant physique* qui agit pour le compte d'un *participant logique* gère les transferts de messages entrant et sortant pour ce *participant logique*.
Participant physique	*Participant* mentionné dans la *liste des participants* à sedex et qui dispose d'un adaptateur sedex et d'un certificat individuel.
Proxy service web	Le proxy service web permet aux utilisateurs de services web d'utiliser localement un protocole non sécurisé pour effectuer des requêtes auprès d'un prestataire de service sécurisé.
RdH	Registre des habitants
Wrapper	Logiciel permettant de démarrer le client sedex en tant que service Windows.

2 Architecture sedex

2.1 Introduction

L'architecture de sedex est basée sur le concept d'applications reliées de manière libre, qui échangent des messages asynchrones en interconnexion avec une plateforme d'échange de données. On parle dans ce cas d'une architecture "hub and spoke" (concentrateur et rayonnement)[1]. Les scénarios de communication à disposition sont les suivants :

- request / reply[2]
- request sans reply

La base de la plateforme d'échanges sedex est fondée sur un intermédiaire implémenté selon un standard OSCI (voir [1] et [2]) défini en Allemagne. L'intermédiaire est un système serveur de communication qui ne connaît pas le contenu du message échangé et qui répond aux exigences de sécurité end-to-end fixées par le législateur (authentification, contrôles d'accès, confidentialité, intégrité des données, retrait des données).

Les messages échangés via la plateforme d'échange de données sont composés d'une enveloppe et de données utiles. L'enveloppe est constituée d'un document XML qui contient les informations d'adressage nécessaires au bon acheminement du message. Les données utiles sont contenues dans un fichier dont le format est défini par le service responsable du type de message.

L'adressage des messages en interconnexion est effectué à partir d'une liste des participants au système. Le système sedex construit à cet effet, selon les cas concrets, des noms "logiques" (commune, service administratif) sur la base des certificats requis pour le transport sécurisé des données.

L'interface des systèmes des applications participantes lors de l'interconnexion avec le système sedex repose principalement sur deux répertoires enregistrés sur le système. L'application doit simplement mettre à disposition les messages à envoyer comme fichiers dans l'un de ces répertoires ; il peut lire les messages qu'il a reçus à partir de fichiers enregistrés dans l'autre répertoire. Les quittances d'envoi du système sont également transmises sous forme de fichiers. Un adaptateur s'occupe d'assurer le transport via le système sedex (voir Illustration 1: Interface entre application et système sedex) .

Outre la fonction centrale de sedex, qui consiste à garantir l'échange asynchrone, sûr et fiable d'importants volumes de données, sedex gère les appels synchrones vers les services web qui acceptent les certificats d'authentification de participants sedex (voir chapitre 3.11).

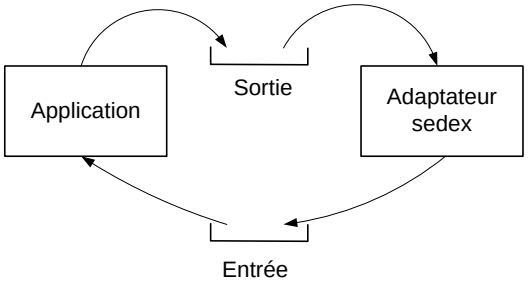


Illustration 1: Interface entre application et système sedex

[1] Concentrateur = Hub, applications= Spoke. Voir aussi http://fr.wikipedia.org/wiki/Hub_and_spoke
[2] Voir aussi http://en.wikipedia.org/wiki/Request-response

2.2 Composants de l'architecture

2.2.1 Vue d'ensemble

L'illustration ci-après donne une vue d'ensemble de l'architecture globale de sedex.

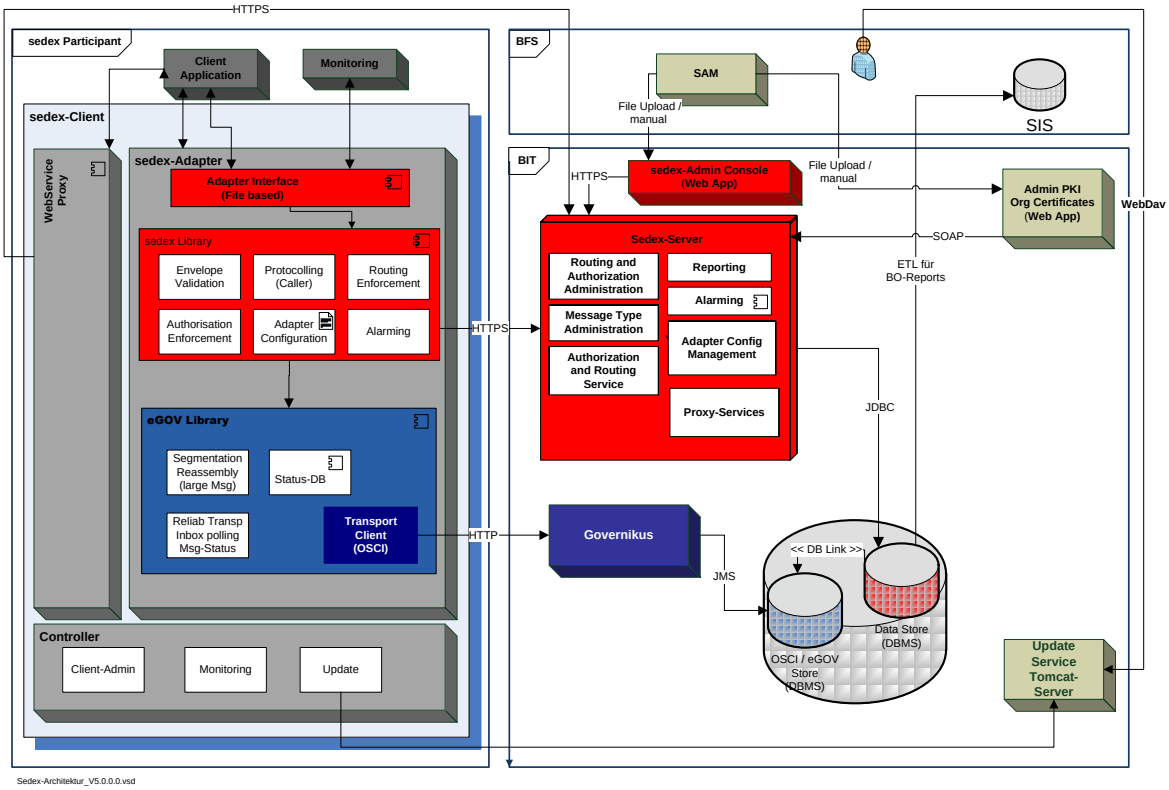


Illustration 2: Architecture globale de sedex

2.2.2 Le serveur sedex

Dans le cadre de l'architecture globale de sedex, le serveur sedex est responsable des tâches suivantes :

- préparation de l'information nécessaire pour le routing des messages
- autorisation de la distribution des messages
- enregistrement centralisé (protocole) de l'ensemble du trafic des messages

2.2.3 Liste des participants

La liste des participants recense tous les participants connus dans l'échange par interconnexion sedex. La liste des participants précise qui peut envoyer quels messages, à qui et comment. Les participants peuvent être actifs ou inactifs. Seuls les participants actifs peuvent envoyer et recevoir des messages.

2.2.4 L'adaptateur sedex

L'adaptateur fonctionne de manière bidirectionnelle, ce qui veut dire qu'il peut aussi bien faire fonction d'émetteur que de récepteur de messages sedex. L'adaptateur envoie et reçoit aussi bien des messages entre les applications communiquant avec sedex que des messages administratifs (c'est-à-dire des messages entre les adaptateurs, respectivement entre l'adaptateur et d'autres composants de l'infrastructure sedex, par ex. le serveur sedex).

Dans l'architecture, l'adaptateur assume les tâches suivantes :

- Surveillance d'un répertoire dans le système de fichiers, dans lequel l'application émettrice inscrit les messages envoyés. Dès que l'adaptateur détecte un message, celui-ci est envoyé.
- Vérification des autorisations (l'application émettrice est-elle habilitée à envoyer des messages à l'application réceptrice ?) et recherche des informations nécessaires au routing d'un message (certificats) auprès du serveur sedex.
- Envoi d'un message au destinataire désigné selon les informations requises par le routing. Le message est signé par l'adaptateur, chiffré avec les certificats du destinataire et, en utilisant la bibliothèque OSCI, transmis à l'intermédiaire OSCI.
- Répétition multiple de l'envoi (retry mechanism), lorsqu'un problème technique surgit (par ex. des perturbations au niveau du réseau).
- Les messages volumineux sont segmentés en vue de l'envoi. Ces segments sont remis ensemble lors de la réception. Cette façon de procéder permet de garantir que lors de grands transferts de données, il n'y ait pas de timeout, notamment lorsque la liaison internet du partenaire de communication ne dispose que d'une faible bande passante.
- Interrogation périodique de la case postale sur l'intermédiaire OSCI.
- Vérification des autorisations (l'application émettrice est-elle habilitée à envoyer des messages à l'application réceptrice ?) et téléchargement des messages depuis la case postale.
- Réception des messages administratifs de la plateforme (Receipts).
- Les messages non attendus sont rejetés.
- Les messages reçus sont déposés par l'adaptateur dans un répertoire du système de fichiers; c'est là que l'application réceptrice peut les récupérer.
- Génération des quittances d'envoi à l'application émettrice.
- Enregistrement centralisé (journalisation) des messages envoyés et reçus.
- L'adaptateur gère sa propre base de données (intégrée), dans laquelle les statuts des messages individuels sont répertoriés. Une sécurité transactionnelle garantit qu'aucun message n'est égaré.

2.2.5 Proxy service web

Le Proxy service web sedex permet aux applications participantes d'utiliser certains services web sans devoir s'auto-authentifier explicitement vis-à-vis du prestataire de service et sans avoir à effectuer le cryptage des données. Sedex procède automatiquement à l'authentification et au cryptage, en utilisant le certificat d'organisation de l'adaptateur. A cet effet, le Proxy service web réplique localement (auprès des clients) les points finaux correspondants du prestataire de service.

Plus d'informations au chapitre 3.11.

2.2.6 Controller

La version 4.0 comprends un controller sedex. Ce produit vient s'ajouter aux composants existants (adaptateur et proxy service web) et est destiné à garantir leur bonne marche.

Principales caractéristiques du controller :

- Surveillance des composants
- Redémarrage des composants lorsque ceux-ci s'arrêtent inopinément
- Mise à disposition d'un monitoring (surveillance du client sedex)
- Extraction à distance des logs et de la configuration pour un meilleur support
- Mise à jour des composants

Jusqu'à la version 3.0, l'adaptateur et le proxy service web sont démarrés de manière indépendante. Dès la version 4.0, seul le controller doit être démarré. A son tour, il démarre l'adaptateur et le proxy service web. De cette façon, le controller détecte et corrige tout arrêt inopiné d'un composant. Le controller apporte donc un changement fondamental dans la manière de démarrer les composants sedex.

2.2.7 Client

Le client sedex n'est pas un programme supplémentaire, mais un terme utilisé à partir de la version 4.0 pour désigner l'installation complète comprenant le controller, l'adaptateur et le proxy service web.

2.3 Scénarios de communication

Dans le processus en interconnexion sedex, émetteur et récepteur sont complètement séparés l'un par rapport à l'autre. La communication entre les deux organes est assurée par un échange de données asynchrone dans lequel le système sedex joue le rôle d'intermédiaire.

L'interface entre l'application et le système sedex est constituée par le répertoire d'entrée et le répertoire de sortie de l'adaptateur.

L'application émettrice prépare les messages à envoyer sous forme de fichiers dans un répertoire de l'adaptateur ; de là, les messages sont transportés par le système sedex vers le ou les destinataires prévus. Les messages destinés à l'application sont réceptionnés par l'adaptateur et mis à disposition dans un répertoire (voir Illustration 1: Interface entre application et système sedex).

Pour chaque message envoyé et pour chaque destinataire de ce message, l'adaptateur établit une quittance d'envoi sous forme d'un fichier XML.

Le Proxy service web propose des services web, permettant des scénarios de communication supplémentaires; nous renonçons à décrire ici ces scénarios, car ils ne font pas partie de la fonction centrale de sedex.

L'illustration 3 montre l'envoi réussi d'un message d'un émetteur à un récepteur. L'adaptateur individuel représenté dans l'illustration résume du point de vue des applications l'ensemble du système sedex.

Pour l'instant, la taille des messages envoyés via ce scénario est limitée à 10 Go. Malgré tout, les expéditeurs doivent être conscients des exigences matérielles que les grands envois peuvent engendrer aussi bien pour l'expéditeur que pour le(s) destinataire(s).

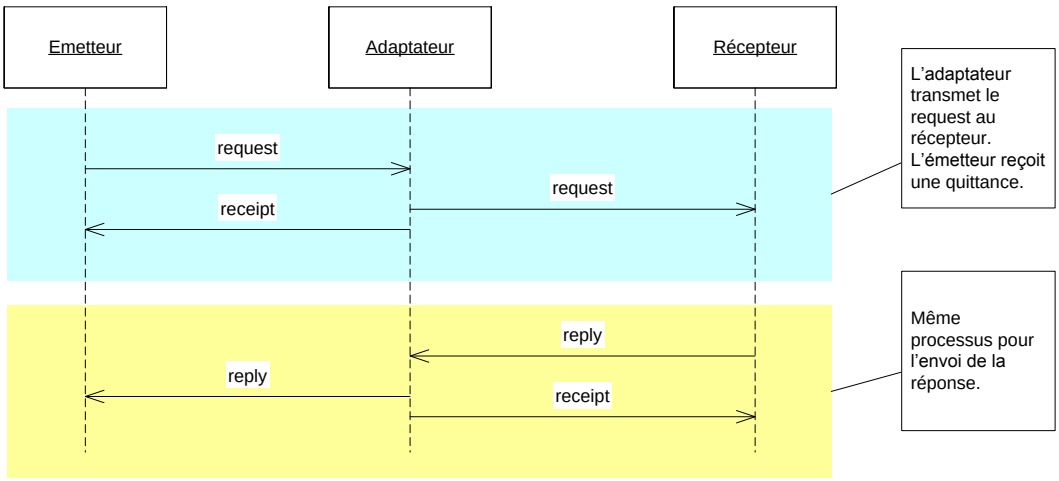


Illustration 3: Envoi réussi d'un message

L'illustration 4 montre l'échec d'un envoi de message. Les causes peuvent résider dans une erreur formelle de l'application émettrice (par ex. adressage erroné dans l'enveloppe) ou dans un problème technique (par ex. problème de réseau). L'application émettrice reçoit dans la quittance d'envoi des indications quant à l'origine de l'erreur.

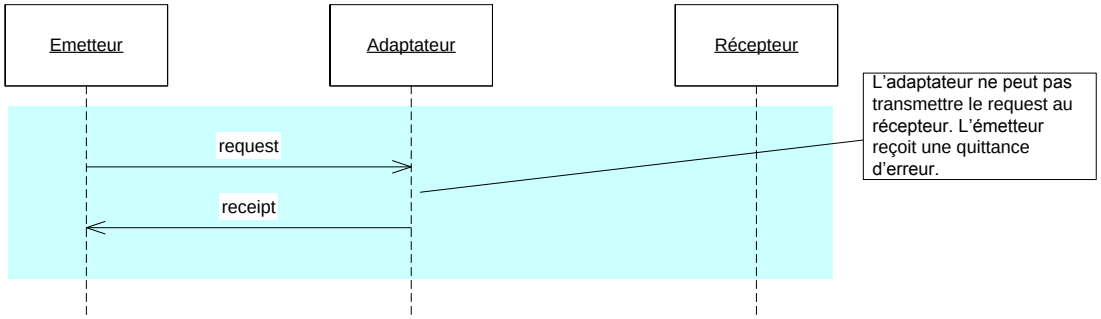


Illustration 4: Envoi non réussi d'un message

L'illustration 5 montre l'envoi d'un seul message à deux destinataires. Ce scénario est réalisé lorsque l'application émettrice mentionne explicitement plusieurs destinataires dans l'enveloppe d'envoi.

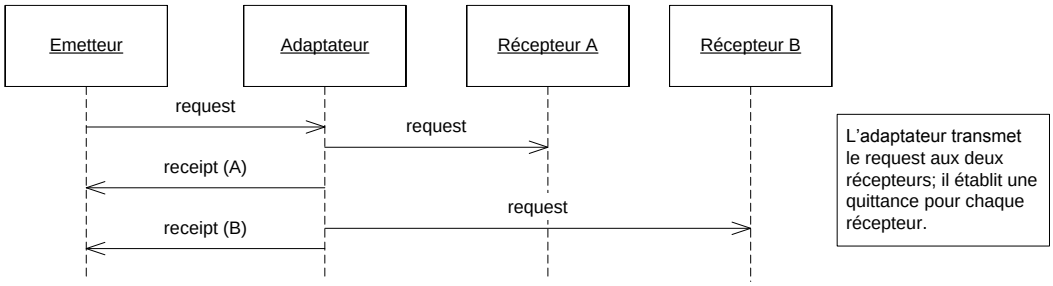


Illustration 5: Envoi d'un message à plusieurs destinataires

2.4 Possibilités de raccordement à sedex

Afin de pouvoir communiquer avec d'autres systèmes et offices connectés au réseau sedex, un logiciel appelé adaptateur sedex est nécessaire. La plateforme sedex différencie les participants sedex et l'adaptateur sedex. Il est ainsi possible de connecter plusieurs participants au réseau sedex à travers un seul adaptateur sedex.

Il existe deux possibilités pour raccorder un participant (p.ex. contrôle des habitants, office des poursuites, etc.) au réseau sedex :

- Raccordement physique
- Raccordement logique

Quel que soit le type de raccordement choisi, chaque participant et chaque adaptateur possède un identifiant sedex (sedex ID). Dans la plupart des cas, le sedex ID d'un adaptateur correspond également au sedex ID d'un participant. En revanche, un participant n'a pas forcément son propre adaptateur. Les deux chapitres suivants expliquent en détail les variantes possibles (physique/logique).

2.4.1 Raccordement physique

Un participant est dit physique lorsqu'il utilise sont propre adaptateur. Dans un tel cas, le sedex ID du participant correspond au sedex ID de l'adaptateur (il n'y a en effet pas lieu de différencier le participant de l'adaptateur, vu que le participant est le seul utilisateur de l'adaptateur en question).

Les participants sedex 1 et 2 dans l'illustration suivante sont des participants physiques.

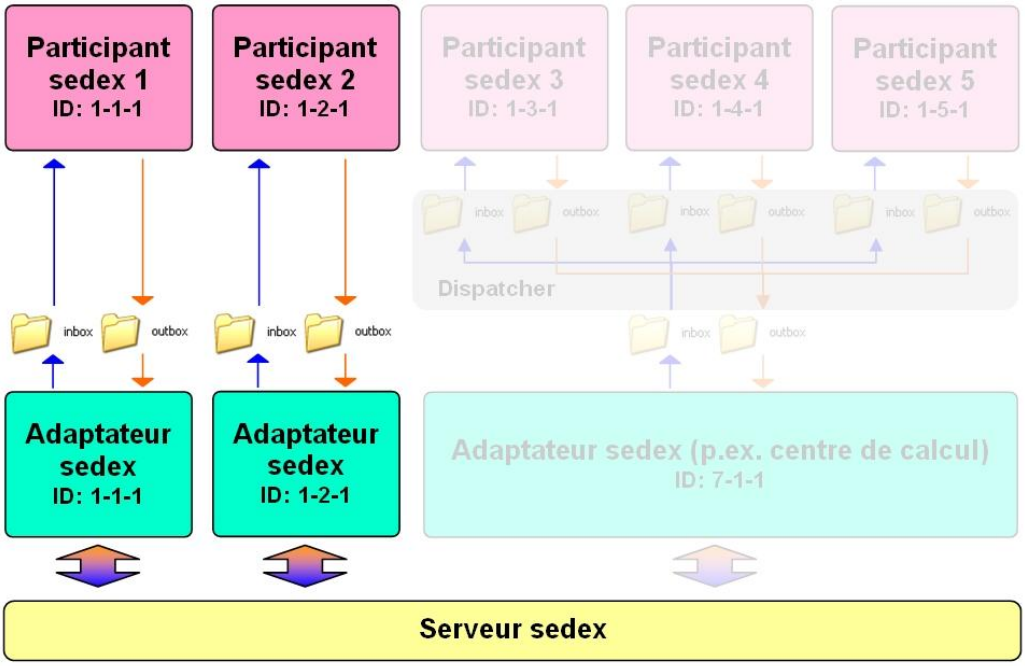


Illustration 6: Exemple de participants physiques

Ce type de raccordement est particulièrement conseillé lorsque le participant à raccorder échange un grand nombre de messages sedex et lorsque les exigences d'isolation (sécurité et protection de l'installation) sont importantes.

Conseil: Afin de garantir une sécurité optimale, il est recommandé d'utiliser un raccordement physique lorsque c'est possible.

2.4.2 Raccordement logique

Un participant est dit logique lorsqu'il utilise un adaptateur générique mis à disposition par un centre de calcul ou un canton. Dans un tel cas, le sedex ID du participant ne correspond pas au sedex ID de l'adaptateur (comme il pourrait y avoir plusieurs participants pour un même adaptateur, une différence est faite entre le participant et l'adaptateur).

L'adaptateur utilisé dans le cadre d'un raccordement logique est le même que celui qui est utilisé pour les raccordements physiques. Il ne propose donc qu'une seule entrée (pour les messages à envoyer) et une seule sortie (pour les messages reçus) alors qu'il pourrait y avoir plusieurs participants logiques utilisant ce même adaptateur. La mise à disposition des messages entrants et la récolte des messages sortants doit être prise en charge par le centre de calcul ou le canton mettant à disposition cet adaptateur commun. Cette tâche est en général exécutée par un programme (un dispatcher).

Les participants sedex 3, 4 et 5 dans l'illustration suivante sont des participants logiques. Les flèches entre ces participants sedex et l'adaptateur correspondant représentent le dispatcher.

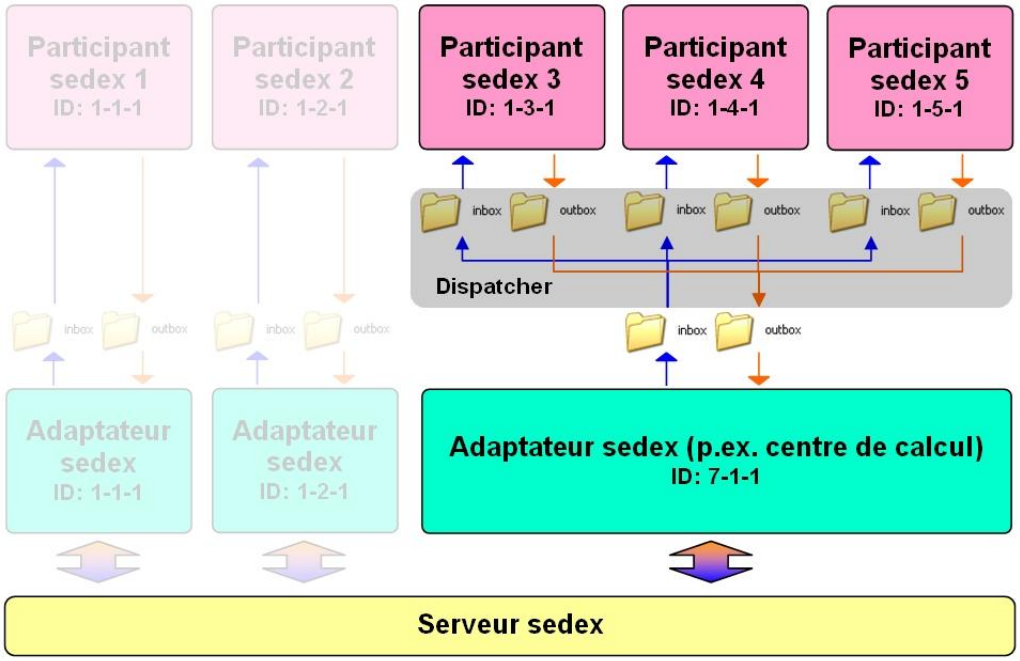


Illustration 7: Exemple de participants logiques

Le dispatcher distribue le courrier entrant au participant sur la base du destinataire (Recipient ID) indiqué dans l'enveloppe sedex, de la même manière que le service postal d'une entreprise distribue le courrier aux employés concernés en fonction du nom indiqué sur l'enveloppe.

Aucun dispatcher n'est proposé par l'OFS ou l'OFIT. Les centres de calculs et les cantons intéressés à proposer un tel service peuvent développer une solution sur mesure ou acquérir une solution disponible sur le marché.

L'exploitant de l'adaptateur sedex répond de la sécurité des données entre les participants logiques et l'adaptateur sedex et veille à ne pas permettre à un participant A l'accès aux données envoyées ou reçues par un participant B.

Ce type de raccordement est idéal pour des centres de calcul désirant proposer une connexion à sedex, sans pour autant devoir exploiter plusieurs adaptateurs sedex. Les participants connectés de cette manière à sedex n'échangent en général que peu de messages sedex.

2.4.3 Indépendance à l'égard de l'adressage des messages

Il est important de garder à l'esprit que le type de raccordement d'un participant n'a aucune influence sur l'adressage des messages. En effet, les éléments sender ID et/ou recipient ID de l'enveloppe (voir chapitre 3.6) peuvent, le cas échéant, être des participants logiques. Les règles de routage du serveur sedex assurent la livraison des messages aux destinataires corrects. Un participant expédiant un message ne doit donc pas savoir si le destinataire est un participant physique (directement raccordé) ou un participant logique (raccordé indirectement via un centre de calcul ou un canton).

3 Utilisation de sedex

3.1 Structure de répertoire du client sedex

L'installation du client sedex nécessite la création d'un nombre conséquent de répertoires. En plus des répertoires d'interface (voir chapitre 3.2.1) qui permettent aux applications participantes d'échanger des données via la plateforme sedex, il existe une multitude d'autres répertoires.

Afin de permettre un fonctionnement optimal, le client sedex doit pouvoir accéder sans restriction à ses répertoires (voir chapitre 4.4.3.2). Pour des raisons évidentes, il est en outre interdit de supprimer des fichiers ou répertoires de l'installation sedex.

La structure de répertoire varie selon la version du client sedex.

3.1.1 Client sedex < V4.0

Ce chapitre donne un aperçu de la structure de répertoire pour les versions < 4.0 du client sedex.

```
sedexclient
├── axis2
├── bin
├── conf
├── deploy
├── inbox
├── internalmessages
├── lib
├── logs
├── messagestorage
├── outbox
├── receipts
├── schema
├── sent
└── zertifikate
```

Répertoire	Description	Contenu
axis2	Contient les fichiers nécessaires pour le fonctionnement du proxy service web (librairies, configuration, fichiers AAR).	sedexclient/axis2 ├── bin ├── conf ├── lib └── repository
bin	Contient les fichiers nécessaires pour démarrer et arrêter le client sedex et installer les services correspondants.	sedexclient/bin ├── InstallAsWindowsService.bat ├── sedexAdapterWrapper.sh ├── start.bat ├── start.sh ├── startwsproxy.bat ├── startwsproxyNoWrapper.bat ├── startwsproxyNoWrapper.sh ├── stop.bat ├── stop.sh ├── UninstallWindowsService.bat ├── wrapper-aix-ppc-32 ├── wrapper-aix-ppc-64 ├── wrapper.exe ├── wrapper-linux-ppc-64 ├── wrapper-linux-x86-32 ├── wrapper-linux-x86-64 ├── wrapper-macosx-ppc-32 ├── wrapper-macosx-universal-32 ├── wrapper-solaris-sparc-32 ├── wrapper-solaris-sparc-64 ├── wrapper-solaris-x86-32

Répertoire	Description	Contenu
		├── wsproxyInstallService.bat ├── wsproxyserver.jar ├── wsproxy.sh ├── wsproxyStartService.bat ├── wsproxyStopService.bat └── wsproxyUninstallService.bat
conf	Contient les fichiers de configuration du client sedex.	sedexclient/conf ├── certificateConfiguration.xml ├── log4j.xml ├── sedexAdapter.properties ├── wrapper.conf ├── wsproxykey.properties ├── wsproxylog4j.properties ├── wsproxy.properties └── wsproxywrapper.conf
deploy	Répertoire utilisé par l'adaptateur sedex, grâce auquel le proxy service web déploie les paquets.	
inbox	Contient les messages entrants (interface entre l'application participante et la plateforme de communication sedex).	
internalmessages	Contient les messages techniques envoyés et reçus.	sedexclient/internalmessages ├── failed ├── incoming ├── outgoing ├── processing ├── sent ├── successful └── unsupported
lib	Contient les librairies nécessaires au fonctionnement du client sedex.	sedexclient/lib ├── activation-1.1.jar ├── adapter.jar ├── alarmingClient.jar ├── annogen-1.0.0.0.jar ├── ant-1.7.0.jar ├── ant-launcher-1.7.0.jar ├── antlr-2.7.6.jar ├── ant-optional-1.5.1.jar ├── asm-1.5.3.jar ├── asm-attrs-1.5.3.jar ├── authorisationClient.jar ├── avalon-framework-4.1.3.jar ├── base64.jar ├── bc.extensions-jdk15-143-bos-0.2.jar ├── bcmail-jdk15-143-bos-0.2.jar ├── bcprov-jdk15-143-bos-0.2.jar ├── bctsp-jdk15-143-bos-0.2.jar ├── bind-2.0.jar ├── buildtime-1.0.0.0.jar ├── certificatechooser.jar ├── CertificateViewer.jar ├── ce_transportimpl.jar ├── cglib-2.1_3.jar ├── ...
logs	Contient les fichiers logs du client sedex.	
messagestorage	Contient les messages à envoyer (Les messages sont déplacés dans ce répertoire dès qu'ils ont été	

Répertoire	Description	Contenu
	enregistrés dans la base de données interne de l'adaptateur).	
outbox	Contient les messages sortants (interface entre l'application participante et la plateforme de communication sedex).	
receipts	Contient les quittances (interface entre l'application participante et la plateforme de communication sedex).	
schema	Contient les schémas XML et les fichiers WSDL nécessaires au fonctionnement du client sedex.	sedexclient/schema ├── AlarmingWebService.wsdl ├── CertificateConfiguration-1-0.xsd ├── CertificateDelivery.xsd ├── CertificateInstallationResult.xsd ├── CertificatePublicationResult.xsd ├── CertificateRenewalAuthorizationStatus.xsd ├── CertificateRenewalGlobalDefinitions.xsd ├── CertificateRenewalInitiation.xsd ├── CertificateRenewalRequest.xsd ├── CertificateRenewalTermination.xsd ├── CheckSedexWebService.wsdl ├── clientServicesTypes.xsd ├── clientServices.wsdl ├── ConfigurationWebService.wsdl ├── eCH-0090-1-0.xsd ├── eCH-0090-2-0.xsd ├── SedexAuthorisationImpl.wsdl ├── sedexServiceMessages-1-0.xsd ├── sedexUtil-1-0.xsd ├── trustStoreDelivery-1-0.xsd ├── xenc-schema.xsd └── xmldsig-core-schema.xsd
sent	Contient les messages traités (pas nécessairement envoyés).	
zertifikate	Contient le certificat d'organisation, le certificat de transport et les truststores.	sedexclient/zertifikate └── prod-bit

3.1.2 Client sedex ≥ V4.0

Ce chapitre donne un aperçu de la structure de répertoire pour les versions ≥ 4.0 du client sedex.

```
sedexclient
├── adapter
├── bin
├── controller
├── interface
├── lib
├── logs
├── monitoring
├── sil
└── temp
```

Répertoire	Description	Contenu
adapter	Contient l'adaptateur sedex, le proxy service web sedex, la base de données interne, les fichiers de configuration, les schémas XML, le certificat d'organisation, le certificat de transport et les truststores.	sedexclient/adapter ├── axis2 ├── bin ├── certificate ├── conf ├── deploy ├── eGovTmp ├── h2db ├── internalmessages ├── jce ├── lib └── schema
bin	Contient les fichiers nécessaires pour démarrer et arrêter le client sedex et installer le service correspondant.	sedexclient/bin ├── controller-InstallAsWinService.bat ├── controller-start.bat ├── controller-start.sh ├── controller-stop.bat ├── controller-stop.sh ├── controller-UninstallWinService.bat ├── controller-wrapper.sh ├── wrapper-aix-ppc-32 ├── wrapper-aix-ppc-64 ├── wrapper.exe ├── wrapper-linux-ppc-64 ├── wrapper-linux-x86-32 ├── wrapper-linux-x86-64 ├── wrapper-macosx-ppc-32 ├── wrapper-macosx-universal-32 ├── wrapper-solaris-sparc-32 ├── wrapper-solaris-sparc-64 └── wrapper-solaris-x86-32
controller	Contient le controller sedex, les fichiers de configuration, le schémas XML et le certificat de mise à jour.	sedexclient/controller ├── backup ├── certificates ├── conf ├── download ├── lib ├── schema └── temp
interface	Contient les répertoires qui forment l'interface entre l'application participante et la plateforme de communication sedex.	sedexclient/interface ├── inbox ├── outbox ├── processed ├── receipts └── sedextempmessage
lib	Contient les librairies nécessaires à l'installation et au démarrage du client sedex en tant que service.	sedexclient/lib ├── libwrapper-aix-ppc-32.a ├── libwrapper-aix-ppc-64.a ├── libwrapper-linux-ppc-64.so ├── libwrapper-linux-x86-32.so ├── libwrapper-linux-x86-64.so ├── libwrapper-macosx-ppc-32.jnilib ├── libwrapper-macosx-universal-32.jnilib ├── libwrapper-solaris-sparc-32.so ├── libwrapper-solaris-sparc-64.so ├── libwrapper-solaris-x86-32.so ├── wrapper.dll └── wrapper.jar
logs	Contient les fichiers logs pour le controller sedex, l'adaptateur sedex et le proxy service web.	sedexclient/logs ├── adapter ├── controller └── wsproxy
monitoring	Contient le fichier d'état généré par le monitoring du controller sedex.	sedexclient/monitoring └── monitoring.txt
sil	Contient des fichiers de verouilla-	sedexclient/sil ├── DO_NOT_DELETE.TXT

Répertoire	Description	Contenu
	ge (“Single Instance Lock”) qui empêchent le double démarrage d’une application.	├── adapter.sil ├── controller.sil └── wsproxy.sil
Temp	Dossier temporaire utilisé notamment par l’assistant d’installation.	

3.2 Interface entre l’application et l’adaptateur

L'application émettrice et l'application réceptrice, dénommées ci-après «émetteur» et «récepteur», sont complètement séparées l’une de l’autre dans le système en interconnexion sedex. La communication entre elles est assurée par un échange de message asynchrone dans lequel le système sedex joue le rôle d’intermédiaire.

L’interface des applications métier participant aux échanges avec le système sedex consiste pour l’essentiel en deux répertoires abrités par le système de fichier, au moyen desquels les fichiers vont être échangés. L’application métier doit simplement pouvoir déposer les messages à envoyer dans l’un de ses répertoires et lire les fichiers correspondant à des messages reçus dans l’autre répertoire.

Les quittances d’envoi du système (« quittances techniques ») sont également préparées sous forme de fichiers. La quittance d’envoi est déposée dans le répertoire "Receipts".

L’adaptateur (voir Illustration 1: Interface entre application et système sedex) assure la transmission via le système sedex.

Un *message* est toujours constitué de deux fichiers:

- Un fichier correspondant à l’*enveloppe*.
  Le fichier de l’enveloppe est un document XML correspondant au schéma XML eCH-0090.xsd et comportant un élément /eCH-0090:envelope. L’adaptateur sedex vérifie le contenu de l’enveloppe du point de vue syntaxique (respect du schéma XML) et sur le plan sémantique (par ex. examiner si l’adresse est correcte, etc.). Seule la version 1.0 du schéma XML eCH-0090 peut être utilisée pour l’enveloppe.
- Un fichier contenant les *données utiles*.
  Le fichier des données utiles peut contenir des données de toutes sortes. L’adaptateur sedex ne procède à aucun contrôle du contenu du fichier des données utiles. Il revient à l’émetteur de vérifier et de garantir que le contenu du fichier soit correct, respectivement au récepteur d’en vérifier le contenu avant tout traitement ultérieur. Si une application souhaite envoyer plusieurs fichiers dans un seul message, il peut le faire en recourant à un fichier zippé ou sous une autre forme compactée. Le type de compactage utilisé doit être réglé entre les applications qui souhaitent échanger des données.

Une *quittance d’envoi* (ou simplement quittance) consiste en un document XML correspondant au schéma XML eCH-0090.xsd et contenant un élément /eCH-0090:receipt. La quittance d’envoi informe si le message a bien été réceptionné par l’adaptateur du récepteur, respectivement si une erreur de transmission a éventuellement eu lieu. La quittance n’est cependant pas une confirmation que le récepteur a bien traité le message. Pour ce faire, les applications doivent convenir de quittances métier spécifiques entre eux. Les versions 1.0 et 2.0 du schéma eCH-0090 peuvent être utilisées pour la quittance.

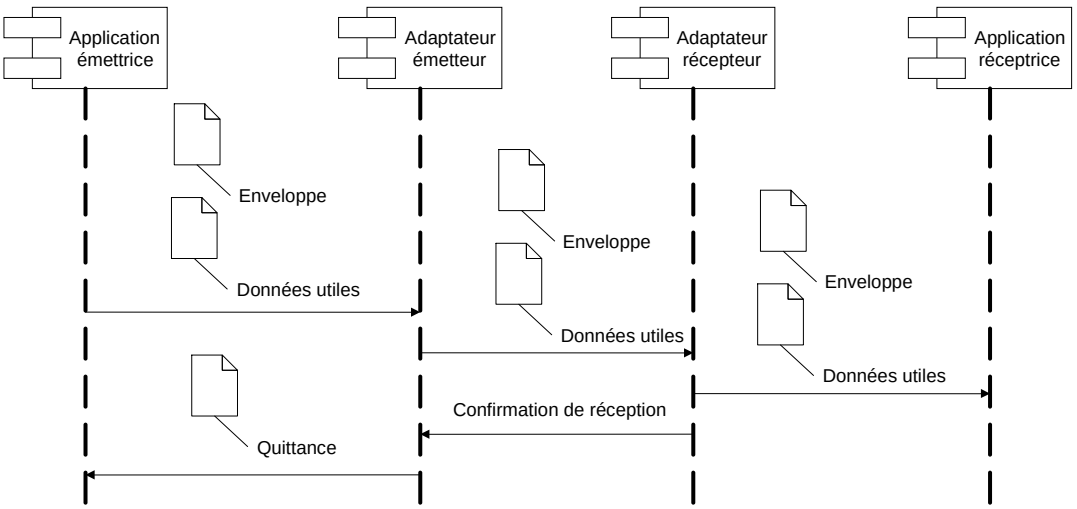


Illustration 8: Déroulement de l'envoi

3.2.1 Répertoires d'interface

Le client sedex nécessite un certain nombre de répertoires pour pouvoir fonctionner. Seulement quatre répertoires sont spécifiquement destinés à l'échange des messages (envoi/réception) et la gestion des quittances. Selon la version de l'adaptateur, les répertoires se trouvent à la racine de l'installation ou dans un sous-répertoire.

Client sedex < V4.0:

- outbox (les messages à envoyer)
- inbox (les messages reçus)
- sent (les messages traités)
- receipts (les quittances sedex)

Client sedex ≥ V4.0**:**

- interface/outbox (les messages à envoyer)
- interface/inbox (les messages reçus)
- interface/processed (les messages traités)
- interface/receipts (les quittances sedex)

3.3 Echange de messages

3.3.1 Envoi d'un message sedex

Lors de l'envoi d'un message, l'adaptateur sedex effectue les traitements dans l'ordre suivant:

1. L'émetteur transmet son message, composé d'une enveloppe et d'un fichier de données utiles, à l'adaptateur en vue de l'envoi. L'application place les fichiers dans le répertoire de sortie de l'adaptateur (répertoire outbox).
2. L'adaptateur balaye en permanence (intervalle de 30 secondes) le dossier outbox (polling), détecte le message, valide l'enveloppe par rapport au schéma XML et stocke le message dans le répertoire *messagestorage* (< V4.0) ou *sedextempmessage* (≥ V4.0).
3. Connexion au serveur sedex pour contrôler les données des participants (actifs, certificat, autorisation, etc.).
4. Les fichiers du message sont déplacés dans le répertoire temporaire de l'adaptateur en vue de l'envoi et segmentés le cas échéant (message > 5 Mo).
5. Le message est signé par l'adaptateur, chiffré avec le certificat du destinataire et transmis au serveur sedex.
6. Les fichiers du message sont déplacés dans le répertoire *sent* (< V4.0) ou *processed* (≥ V4.0) pour archivage, indépendamment de l'état d'envoi.
7. Dès que le destinataire a téléchargé le message, l'adaptateur génère une quittance technique[4] par destinataire avec le statut d'envoi. Cette quittance est mise à disposition de l'application émettrice par l'intermédiaire du répertoire *receipts*.
8. L'application récupère et interprète la quittance.

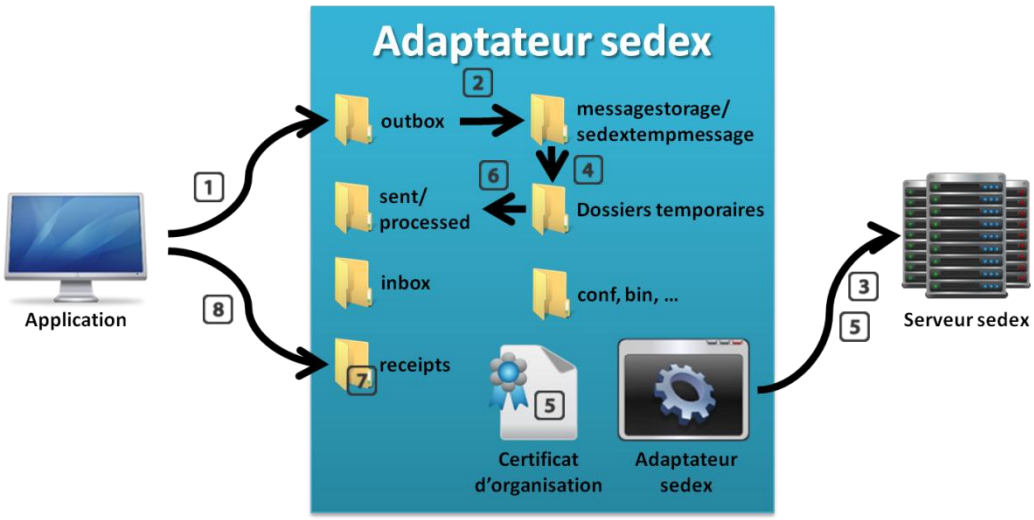


Illustration 9: Processus d'envoi

Si le destinataire envoie une réponse en retour à l'émetteur, le déroulement décrit ci-dessus se répète à l'identique, mais avec des rôles inversés.

[4] L'adaptateur établit également des quittances de mise à jour de statut et des avertissements pendant le processus de transmission.

3.3.2 Réception d'un message sedex

Lors de la réception d'un message, l'adaptateur sedex effectue les traitements dans l'ordre suivant:

1. Surveillance de la boîte postale sur le serveur sedex (voir chapitre 3.14)
2. Téléchargement partiel du message dans le répertoire temporaire
3. Contrôles de sécurité (signature, chiffrement, autorisation)
4. Poursuite du téléchargement dans le répertoire temporaire
5. Dès que le fichier est déchiffré, il est déplacé dans le répertoire inbox
6. Le statut du message est mis à jour sur le serveur sedex et une quittance technique est adressée à l'émetteur.

3.4 Convention d'écriture

L'adaptateur émetteur attend les fichiers suivants :

L'enveloppe en tant que fichier envl_N.xml

Les données utiles en tant que fichier data_N.xxx

«N» est un suffixe nominal univoque produit par l'application. La corrélation entre l'enveloppe et les données utiles est assurée par l'utilisation de suffixes identiques. Par exemple, les fichiers envl_4711.xml et data_4711.zip constituent un message car ils contiennent le même suffixe 4711. En dehors de la corrélation entre enveloppe et données utiles, les noms des fichiers n'ont pas de signification pour l'adaptateur. L'application est donc libre de générer ces suffixes selon ses propres besoins. Nous recommandons cependant d'utiliser le messageId de l'enveloppe comme suffixe nominal.

«xxx» représente une extension de fichier correspondant au type de fichier utilisé (XML, ZIP, PDF, etc.). L'adaptateur déduit le type de fichier à partir de cette extension.

L'adaptateur émetteur place la quittance d'envoi sous forme d'un fichier dénommé "receipt__ID_M_Y.xml" dans le répertoire de quittance. "M" y représente le *messageID* et "Y" un numéro séquentiel univoque attribué par l'adaptateur. L'adaptateur établit une quittance d'envoi pour chaque récepteur explicitement mentionné dans l'enveloppe et à qui il a envoyé un message. Lorsque deux récepteurs sont mentionnés dans l'enveloppe, l'émetteur reçoit donc deux quittances d'envoi.

L'adaptateur récepteur établit les fichiers suivants lorsqu'il reçoit un message :

L'enveloppe en tant que fichier «envl_M.xml»

Les données utiles en tant que fichier «data_M.xxx»

«M» représente un code alphanumérique séquentiel univoque généré par l'adaptateur de réception. La corrélation entre l'enveloppe et les données utiles est donnée par l'attribution de codes séquentiels alphanumériques identiques.

Lors du transport, les noms de fichiers **ne sont pas conservés**. Seule l'extension de fichier du fichier des données utiles est conservée car elle désigne le type de fichier. Si une application a besoin de ce nom de fichier pour une raison quelconque, le fichier original doit alors être transmis sous forme de fichier zippé.

3.5 Mise à disposition de messages

Un message est considéré comme prêt à l'envoi (de l'émetteur à l'adaptateur d'émission), respectivement au traitement ultérieur (de l'adaptateur de réception au récepteur) lorsque le fichier de l'enveloppe est déposé dans le répertoire correspondant.

La stratégie suivante, indépendante de la plateforme, doit être utilisée, pour éviter des interférences :

- Générer le fichier des données utiles selon les conventions d'écriture dans le répertoire correspondant et y inscrire les données.
- Générer le fichier de l'enveloppe sous forme de fichier temporaire dans le répertoire correspondant avec un nom qui n'est pas identique au nom final de l'enveloppe selon les conventions d'écriture (par ex. "tmp<processid>.xml"). Inscrire les données de l'enveloppe dans le fichier.
- Renommer le nom du fichier de l'enveloppe selon les conventions d'écriture.

3.6 Contenu de l'enveloppe

L'enveloppe d'un message sedex contient les éléments suivants, conformément au schéma XML eCH-0090 :

Nom de l'élément	Signification	Type	Oblig.	Nombre
messageId	**Application émettrice** Cet ID est attribué par l'application émettrice. Le message ID doit être univoque dans le contexte de celle-ci. Il permet à l'application émettrice de corréler un message avec sa réponse. Si plusieurs applications se partagent un adaptateur, une convention de distribution des messages ID doit exister entre les applications participantes (notion de range). L'unicité du couple (sender ID / message ID) doit être gérée par l'application émettrice. **Adaptateur sedex** Dans le contexte du système sedex, le couple (Sender ID, Message ID) n'est pas toujours univoque (voir chapitre 3.9.4).	String, correspondant à l'expression régulière : ([a-zA-Z] | [0-9] | -){1,36} Soit une chaîne de caractères de max. 36 caractères pouvant comprendre des chiffres, des lettres ou des traits d'union. La suite de signes est assez longue pour représenter un UUID (voir RFC 4122), un 64 bit integer ou un type de clé. Exemple : f81d4fae-7dec-11d0-a765-00a0c91e6bf6	Oui	1
messageType	Type de message. Le type définit la fonction d'un paquet de données. La plage de valeur disponible est divisée en sous-plages. Les sous-plages sont attribués à des domaines métiers précis. La signification des différents types de messages est décrite dans le document [9]. Avec la classe de message (messageClass), le type de message définit implicitement la catégorie des données utiles du message (type de fichier, resp. schéma XML). Avec le senderId et le recipientId, le type de message est déterminant pour le routing du message.	[0 ... 2699999] (sous-ensemble de xs:int)	Oui	1

Nom de l'élément	Signification	Type	Oblig.	Nombre
messageClass	Classe de message. Définit dans le cadre du type de message la signification du message. Les valeurs suivantes sont prédéfinies : • 0 = message. Marque le message initial. • 1 = response. Marque la réponse à un message. • 2 = receipt. Marque la quittance par une application (confirmation de réception), que le récepteur envoie à l'application émettrice. Le cas échéant, une quittance de ce type est envoyée lorsqu'un grand laps de temps peut s'écouler d'ici à l'envoi d'une réponse ou lorsque le récepteur n'a pas prévu d'envoyer de réponse. • 3 = Error. Information de l'application destinataire à l'attention de l'application émettrice indiquant que le message n'a pas pu être traité. • 4 - 9 et 11 - maxint: réservé pour des développements ultérieurs.	xs:int	Oui	1
referenceMessageId	Cet élément est attribué par une application en réponse à une autre application ou lorsqu'elle émet un message d'erreur par rapport à un message. L'élément contient l'ID du message initial. Cet élément doit être placé lorsque messageClass = 1 (response), = 2 (receipt) ou = 3 (error).	Idem que pour messageId	Non	1
senderId	Emetteur du message. Désigne de manière univoque le service administratif qui émet le message.	String. Constitué selon chapitre 3.8.	Oui	1
recipientId	Récepteur du message. Désigne de manière univoque le service administratif qui reçoit le message.	String. Constitué selon chapitre 3.8.	Oui	>0
eventDate	Date de l'événement. Date à laquelle l'événement auquel se réfèrent les données utiles s'est produit. La date de l'événement peut être considérée comme partie intégrante des données utiles par le récepteur (par ex. déménagement, jour de référence dans la livraison pour la statistique, etc.).	xsd:dateTime	Oui	1

Nom de l'élément	Signification	Type	Oblig.	Nombre
messageDate	Date d'envoi. Date (chronotimbre), à laquelle l'application émettrice a déposé le message dans le répertoire de sortie de l'adaptateur.	xsd:dateTime	Oui	1
loopback	Marque le message en tant que message de loopback. Un loopback est un message que l'adaptateur de réception traite comme un message normal (le cas échéant, la légitimité de l'émetteur est vérifiée) mais qu'il ne transfère pas dans son application. Ce genre de message est aussi utilisé en exploitation pour effectuer des tests.	Modèle de contenu vide avec un attribut ‚authorise'. L'attribut définit si le contrôle de légitimité sedex doit être effectué pour ce message loopback. Si la valeur est positionnée sur "true", le message peut être utilisé pour vérifier si un émetteur est bien habilité à envoyer un message d'un certain type à un récepteur. Si la valeur est positionnée sur "false", le message peut être utilisé comme simple test de liaison entre deux adaptateurs (ping).	Non	0,1
testData	Peut être utilisé par une application émettrice pour des tests, afin d'actionner la simulation de la réception. La sémantique des valeurs transmises est l'affaire du simulateur de réception	Couple noms/valeurs	Non	>=0

Le document XML suivant montre un exemple d'enveloppe :

```
<?xml version="1.0" encoding="UTF-8"?>
<envelope xmlns="http://www.ech.ch/xmlns/eCH-0090/1"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ech.ch/xmlns/eCH-0090/1
http://www.ech.ch/xmlns/eCH-0090/1/eCH-0090-1-0.xsd"
  version="1.0">
  <messageId>62fdee70d9ea77646f6e8686a3f9332e</messageId>
  <messageType>99</messageType>
  <messageClass>0</messageClass>
  <senderId>1-351-1</senderId>
  <recipientId>3-CH-1</recipientId>
  <eventDate>2007-01-01T00:00:00</eventDate>
  <messageDate>2007-09-06T14:13:51</messageDate>
</envelope>
```

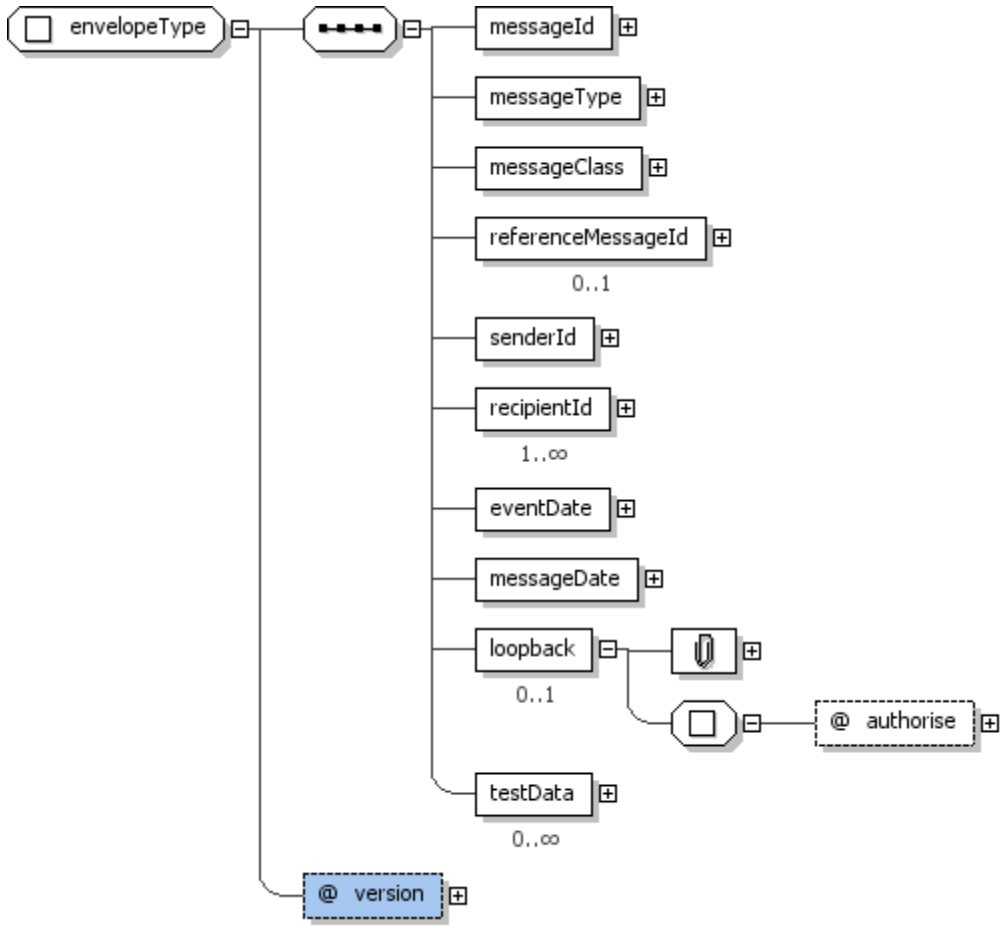


Illustration 10: Représentation graphique du modèle pour le contenu de l'enveloppe

3.7 Contenu de la quittance

La quittance est produite par l'adaptateur pour chaque destinataire d'un message. Ainsi, si l'émetteur envoie un message à deux récepteurs, il reçoit en retour deux quittances.

La quittance contient les éléments suivants:

Nom élément	Signification	Type	Oblig.	Nombre
eventDate	Moment de l'événement qui a conduit à la quittance. Par ex. heure d'arrivée du message dans l'adaptateur récepteur ou heure à laquelle une erreur de transmission s'est produite.	xsd:dateTime	Oui	1
statusCode	Statut du message : ok ou code d'erreur.	Enumération sur la base de xsd:int Valeurs possibles voir chapitre 3.9.	Oui	1
statusInfo	Texte d'information sur le code de statut. Contient éventuellement des informations qui peuvent intéresser les administrateurs du système.	xsd:string, maxlength=255 Valeurs possibles voir chapitre 3.9.	Oui	1
messageId	ID du message auquel la quittance se réfère.	Idem que dans l'enveloppe	Oui	1
messageType	Type de message du message auquel la quittance se réfère.	Idem que dans l'enveloppe	Oui	1
messageClass	Classe de message du message auquel la quittance se réfère.	Idem que dans l'enveloppe	Oui	1
senderId	Emetteur du message auquel la quittance se réfère.	Idem que dans l'enveloppe	Oui	1
recipientId	Récepteur du message auquel la quittance se réfère.	Idem que dans l'enveloppe. A relever que dans la quittance apparaît toujours le recipientId tel qu'il a été indiqué dans l'enveloppe. Et cela même si l'adaptateur achemine le message à un autre récepteur sur la base des règles de routing (par ex. une plateforme centralisée cantonale).	Oui	1

Le document XML suivant montre un exemple de quittance d'envoi d'un message transmis avec l'enveloppe décrite au chapitre précédent et qui est bien parvenu au récepteur.

```
<?xml version="1.0" encoding="UTF-8"?>
<receipt xmlns="http://www.ech.ch/xmlns/eCH-0090/1"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ech.ch/xmlns/eCH-0090/1
http://www.ech.ch/xmlns/eCH-0090/1/eCH-0090-2-0.xsd"
  version="2.0">
  <eventDate>2007-09-06T14:13:51Z</eventDate>
  <statusCode>100</statusCode>
  <statusInfo>OK</statusInfo>
  <messageId>62fdee70d9ea77646f6e8686a3f9332e</messageId>
  <messageType>99</messageType>
  <messageClass>0</messageClass>
  <senderId>1-351-1</senderId>
  <recipientId>3-CH-1</recipientId>
</receipt>
```

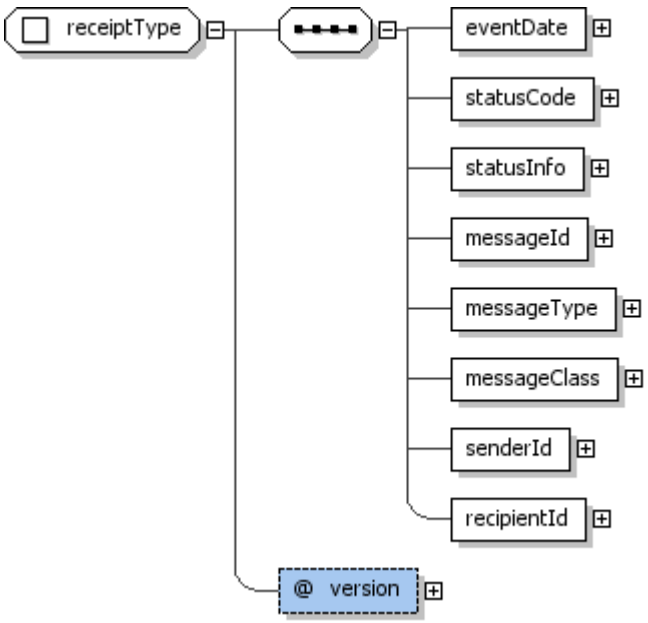


Illustration 11: Représentation graphique du modèle pour le contenu d'une quittance

3.8 Adressage

3.8.1 Vue d'ensemble

Les participants à l'interconnexion sedex sont par exemple les systèmes des services administratifs des communes, des cantons et de la Confédération. Ils sont identifiés par un ID univoque. Pour permettre aux systèmes participant de générer facilement l'adressage des partenaires dans l'interconnexion, le système sedex définit un ID de participant construit logiquement. Le système sedex construit cet ID de participant sur la base de la liste des participants et du certificat qui est attribué à un participant concret.

L'ID participant est une chaîne de caractères[5], construite de la manière suivante :

ID participant = <niveau institutionnel> "-" <unité organisationnelle> "-" <code de fonction>.

3.8.2 Niveaux institutionnels et unités organisationnelles

Les numéros des niveaux institutionnels définissent un "espace nominatif" dans le domaine d'adressage de sedex. A l'intérieur d'un de ces niveaux institutionnels, des unités organisationnelles individuelles peuvent ensuite être définies.

Niveau	Signification	Plage de valeur pour l'unité organisationnelle
0	sedex Niveau réservé pour le système sedex. Sert à l'adressage des services internes de sedex.	Seule valeur possible : sedex
1	Commune Désigne une commune.	Les valeurs admises sont les numéros OFS des communes politiques selon [3], par ex. 351 pour Berne.
2	Canton Désigne un canton.	Les valeurs admises sont les abréviations à deux lettres des cantons selon [3], par ex. SO pour Soleure.
3	Confédération Désigne un office fédéral ou une application de la Confédération.	Unique valeur possible: CH
4	EBS-Dir. Désigne l'annuaire des participants Event Bus Suisse.	
5	District Désigne un district dans un canton.	Les valeurs admises sont les numéros OFS des districts selon [3].
6	Institutions d'assurances sociales	Numéro à 6 positions délivré par l'office fédéral des assurances sociales (OFAS) aux caisses de

[5] Aujourd'hui, la longueur de l'ID participant est limitée à 20 caractères pour des raisons techniques. A l'avenir, cette limitation devrait cependant tomber.

Niveau	Signification	Plage de valeur pour l'unité organisationnelle
	Désigne une caisse de compensation AVS ou un office AI.	compensation/filiales AVS, aux offices AI et PC, à l'armée et aux milieux intéressés.
7	Entreprise privée Désigne un participant de droit privé.	Les valeurs admises sont attribuées par OFS aux entreprises privées participant à sedex. Ces numéros ne sont pas parlant . p. ex. 1 pour TI Informatique
8	e-LP Désigne les offices de poursuites et les créanciers membres de l'interconnexion e-LP.	Les valeurs admises sont les abréviations à deux lettres des cantons selon [3], par ex. SO pour Soleure.
9	réservé	

Dans la liste des participants sedex, il est possible de distinguer des participants qui ne servent qu'à des fins de test. L'ID de ces participants est muni d'un préfixe "T". De tels participants peuvent uniquement communiquer entre eux.

3.8.3 Code de fonction

Le code de fonction décrit le secteur d'activité du participant.

Les secteurs d'activités, respectivement leur code de fonction, sont définis par domaine, c'est-à-dire qu'un même code de fonction, selon le domaine dans lequel il est utilisé, peut désigner un secteur d'activité différent.

Actuellement, les codes de fonction suivants sont attribués :

3.8.3.1 Domaine système

Domaine	Code de fonction	Secteur d'activité / Signification
0	0	Le système sedex
0	1	Le système de monitoring sedex

Pour les besoins exclusif du système sedex, l'OFS attribue des codes de fonction pour le domaine 0 (sedex).

3.8.3.2 Domaine communal

Domaine	Code de fonction	Secteur d'activité / Signification
1	1	Registre des habitants (RdH)
1	2	Informatique
1	3	Statistique
1	4	-
1	5	Administration fiscale
1	6	Commune bourgeoise

Domaine	Code de fonction	Secteur d'activité / Signification
1	7	-
1	8	Créancier

Les codes de fonction supérieurs à 5 sont réservés pour des fonctions dépassant le niveau communal. A ce titre, ils sont attribués par l'OFS.

3.8.3.3 Domaine cantonal

Domaine	Code de fonction	Secteur d'activité / Signification
2	1	Registre des habitants (RdH)
2	2	Informatique
2	3	Statistique
2	4	Registre du commerce
2	5	Administration fiscale
2	6	-
2	7	Administration militaire
2	8	Créancier
2	9	Office de poursuites

Les codes de fonction 1000 à 26999 du domaine 2 (canton) sont réservés pour des développements ultérieurs réalisés par les différents cantons. La numérotation fonctionne de manière identique au type de message; le préfixe correspond donc au numéro de canton de l'OFS.

Exemple: le canton de Zürich peut librement disposer de la plage de numéro 1000 à 1999 pour ses besoins particuliers.

3.8.3.4 Domaine fédéral

Domaine	Code de fonction	Secteur d'activité / Signification
3	1	Office fédéral de la statistique
3	2	Office fédéral de la statistique (seulement pour utilisation interne)
3	3	CdC UPI DB DMZ
3	4	InfoStar
3	5	SYMIC
3	6	ORDIPRO
3	7	VERA
3	8 – 17	Office fédéral de la statistique (seulement pour utilisation interne)

Les codes de fonction sont réservés pour la Confédération. Ces numéros sont attribués par l'OFS. Un historique est tenu pour ces numéros; un numéro est attribué de façon permanente, et ne pourra plus être réutilisé pour un autre service.

3.8.4 Exemples

- 0-sedex-0 désigne le système sedex lui-même.
- 1-351-1 désigne le RdH de la commune politique de Berne.
- 1-351-6 désigne le RdH de la commune bourgeoise de Berne.
- 2-SO-1 désigne le RdH du canton de Soleure.
- 2-GL-2 désigne le service cantonal de l'informatique de Glaris.
- 3-CH-5 désigne le système central d'information sur les migrations (SYMIC) du DFJP.
- T3-CH-1 désigne l'instance de test de l'Office fédéral de la statistique.
- 7-1-1 désigne l'adaptateur sedex n°1 de l'entreprise TI Informatique.
- 8-TG-1 désigne le premier office de poursuites du canton de Thurgovie connecté à sedex.

3.9 Catégories d'erreurs et codes de statut

Les codes de statut sont subdivisés en catégories et en sous-catégories. Les catégories sont structurées de telle manière que l'application appelante est déjà en mesure de décider, en fonction de la catégorie du code, de la réaction à adopter. Ainsi, dans le cas d'un code de statut *erreur temporaire*, un nouvel envoi peut être tenté après un certain temps.

Une application doit également être capable de réagir à un code inconnu, en le traitant en fonction de sa catégorie d'appartenance ou, le cas échéant, en l'ignorant (en fonction de sa catégorie, p. ex. pour les informations / avertissements).

3.9.1 Catégories d'erreurs

Les codes de statut qui peuvent survenir lors de la transmission sont classés de la manière suivante :

Catégorie	Sous-catégorie	Codes de statut	Explication
Réussite	Ex.: un message a été envoyé avec succès.	100 – 199	Confirmations de la réception **Comportement**: informer l'utilisateur
Erreur permanente	**Message Error** Ex.: l'enveloppe d'un message n'est pas valable	200 – 299	Il y a un problème avec le message ou l'autorisation. Une nouvelle tentative d'envoi sans modification des conditions entraînera la même erreur.
	Authorisation Error	300 - 399	

	Ex.: l'un des récepteurs de l'enveloppe n'a pas l'autorisation requise.		**Comportement**: corriger le problème ou informer l'utilisateur avant un nouvel envoi
Erreur temporaire	**Transport Error** Ex.: le serveur d'autorisation est provisoirement indisponible.	400 – 499	Un problème est apparu au niveau du transport ou des adaptateurs. **Comportement**: renvoyer le message après un certain temps.
	Adapter Error Ex.: l'adaptateur ne dispose pas de suffisamment de mémoire.	500 – 599	
Information	**Update** Ex.: un message a été envoyé avec succès au serveur.	600 – 699	Des informations confirment la progression de l'envoi, mais celui-ci n'est pas encore arrivé à destination. **Comportement**: l'information peut être traitée ou ignorée.
	Avertissement Ex.: le récepteur n'a plus que quelques jours pour télécharger le message.	700 – 799	Un avertissement a été généré suite à l'envoi d'un message. **Comportement**: l'avertissement peut être traité ou ignoré.

3.9.2 Codes de statut

Les codes de statut suivants sont définis pour la quittance :

Sous-catégorie	Valeur	Message correspondant	Signification	Source[6]	Depuis[7]
Success	100	Message correct transmitted	Le message est correct et a été intégralement transmis.	AR	1.0
Message Error	200	Invalid envelope syntax	L'enveloppe ne correspond pas au schéma XML attendu pour les enveloppes, respectivement elle n'est pas dans la version en vigueur. Voir aussi le chapitre 0.	AE AR	1.0

[6] Comme source, l'adaptateur est résumé comme suit :
AE = adaptateur émetteur, AR = adaptateur récepteur.
[7] Le code de statut a été introduit lors du nouveau Release de l'adaptateur.

Sous-catégorie	Valeur	Message correspondant	Signification	Source[6]	Depuis[7]
	201	Duplicate message ID	L'enveloppe contient un ID de message dont l'adaptateur dispose déjà dans sa banque de données des statuts. (voir chapitre 3.9.4)	AE	1.0
	202	No Payload found	Un message sedex se compose toujours de deux fichiers: l'enveloppe et les données (voir chapitre 0). L'application émettrice a mis uniquement à disposition une enveloppe, sans le fichier de données.	AE	1.0
	203	Message to old to send	La date du message dans l'enveloppe remonte à plus de 30 jours.	AE	2.0
	204	Message expired	Le récepteur n'a pas réceptionné le message dans les 30 jours fixés par sedex.	AE	2.0
Autorisation Error	300	Unknown sender id %s	Le senderId donné dans l'enveloppe n'est pas répertorié dans la liste sedex.	AE	1.0
	301	Unknown recipient id %s	Le recipientId donné dans l'enveloppe n'est pas répertorié dans la liste sedex.	AE	1.0
	302	Unknown physical sender id %s	L'ID de l'adaptateur configuré dans l'adaptateur n'est pas répertorié dans la liste sedex (ne peut se produire que dans des infrastructures centralisées).	AE	1.0
	303	Invalid message type %s	Le type de message mentionné dans l'enveloppe n'est pas connu.	AE	1.0

Sous-catégorie	Valeur	Message correspondant	Signification	Source[6]	Depuis[7]
	304	Invalid message class %s	La classe de message mentionnée dans l'enveloppe n'est pas connue.	AE	1.0
	310	Not allowed to send	Cet émetteur n'est pas habilité à envoyer ce message.	AE	1.0
	311	Not allowed to receive	Ce récepteur n'est pas habilité à recevoir ce message. Cela peut arriver lors-qu'après l'envoi, mais avant la réception du message, le routage de l'AR ou l'autorisa-tion du récepteur a été modifié.	AE AR	1.0
	312	User certificate not valide	Le certificat du partici-pant a été annulé ou n'est plus valable	AE	1.0
	313	Other recipients are not allowed to receive	Le message ne peut être envoyé au desti-nataire, car d'autres destinataires égale-ment listés dans l'enveloppe ne sont pas habilités à recevoir ce message.	AE	2.0
	320	Message expired	*Remplacé par 204 à partir de la version 2.0 de l'adaptateur. Voir signification dans la version en question.*	AE	-
	330	Message size exceeds limit	Le message dépasse la taille autorisée pour ce type de message.	AE	2.0
Transport Error	400	Network error	Problème général de réseau.	AE	1.0
	401	OSCI hub not reachable	Aucune liaison avec l'intermédiaire OSCI possible.	AE	1.0
	402	Directory not reachable	La liste sedex n'est pas atteignable.	AE	1.0

Sous-catégorie	Valeur	Message correspondant	Signification	Source[6]	Depuis[7]
	403	Logging service not reachable	Le logging sedex n'est pas atteignable.	AE	1.0
	404	Authorisation service not reachable	Le service d'autorisation de sedex n'est pas disponible.	AE	2.0
Adapter Error	500	Internal error: %s	L'adaptateur ne peut pas envoyer les données car une erreur interne s'est produite. D'autres informations sont rattachées à ce message (remplacer %s). Les détails concernant ces erreurs figurent dans le log de l'adaptateur.	AE	1.0
	501	Error during receiving	Une erreur s'est produite lors de la réception du message, que le récepteur n'a pas pu reconstituer	AR	2.0
Partial Success	601	Message successfully sent	Le message a été remis avec succès à l'intermédiaire.[8]	AE	2.0
Warning	701	Message expires soon	L'adaptateur récepteur a encore 7 jours pour télécharger le message de l'intermédiaire.	AE	2.0

[8] La réception de cette quittance qui confirme l'envoi du message au serveur sedex est paramétrable. Elle est toutefois désactivée par défaut.

3.9.3 Comportement en cas d'enveloppe incorrecte (statut 200)

Si l'application émettrice transmet à l'adaptateur une enveloppe qui n'est pas correcte sur le plan de la syntaxe (l'enveloppe ne peut pas être validée par rapport au schéma eCH-0090 -> Status-code 200), l'adaptateur n'est pas en mesure d'en extraire les éventuelles informations qu'elle peut contenir sur l'émetteur, le récepteur, etc.

C'est également le cas pour les messages reçus dont le fichier d'enveloppe n'est pas compatible avec la version de schéma correspondant à l'adaptateur récepteur.

Dans ce cas, l'adaptateur va produire une seule quittance, quel que soit le nombre de récepteurs mentionné dans l'enveloppe. Cette quittance a les valeurs indiquées ci-après.

L'adaptateur essaie si possible d'identifier le *messageID*, pour simplifier l'analyse de l'erreur. Si cela n'est pas possible, le nom du fichier d'enveloppe est joint dans l'élément "statusInfo".

En résumé, la quittance du statut "200" contient les éléments suivants:

Nom de l'élément	Valeur	Condition
eventDate	Date/heure actuelles	
statusCode	200	
statusInfo	Invalid envelope syntax	messageId <> 0
	Invalid envelope syntax found in file %f	messageId = 0
messageId	0	messageId pas trouvé dans l'enveloppe
	<> 0	messageId trouvé dans l'enveloppe
messageType	0	
messageClass	0	
senderId	0-sedex-0	
recipientId	0-sedex-0	

3.9.4 Gestion des doublons en matière de message ID (statut 201)

L'adaptateur sedex garanti l'unicité du message ID jusqu'à l'arrivée du message à son destinataire. En effet, l'adaptateur stocke en mémoire toutes les informations liées à l'enveloppe sedex jusqu'à l'arrivée du message à destination. Tant que ce message est stocké, aucun autre message portant le même message ID ne sera accepté pour envoi et fera l'objet d'une quittance avec le statut 201.

Après la génération de la quittance technique (pour le message envoyé), il est possible de renvoyer un autre message comportant le même identifiant. Ce nouvel envoi est possible uniquement après l'exécution de la tâche programmée, destinée à vider, régulièrement, la base de données interne de l'adaptateur. L'intervalle dépend du profil choisi (voir chapitre 3.16).

3.9.5 Comportement lors d'erreurs de réseau

L'adaptateur sedex distingue les erreurs permanentes des erreurs temporaires.

Les erreurs de connexion sont typiquement des erreurs temporaires. Si une telle erreur se produit, l'adaptateur essaie régulièrement d'envoyer le message durant la période configurée dans la retry period. Ce n'est qu'à l'issue de ce laps de temps que l'adaptateur va générer une quittance d'envoi avec le statut d'erreur de la catégorie réseau ("network").

A partir de la version 4.0, les différents mécanisme de retry ont été unifiés afin de rendre la durée configurable. La valeur par défaut pour la retry period est de 5 heures. Cette valeur peut être modifiée à l'aide d'un paramètre adéquat dans le fichier de configuration du client sedex (voir document [7]).

Lorsqu'une erreur permanente se produit, l'adaptateur génère immédiatement une quittance d'envoi négative.

3.9.6 Calcul de la date de péremption d'un message (codes de statut 203, 204 et 701)

Les messages doivent être retirés par l'adaptateur destinataire dans un délai d'un mois. Est déterminant l'élément /eCH-0090:envelope/messageDate, indépendamment de la date d'envoi effective.

Pour cette raison, sedex procède aux validations suivantes:

- Lors de l'envoi du message: *messageDate* ne doit pas être plus petit que la date actuelle moins 30 jours ➔ code de statut «203 Message too old to send» à l'adaptateur émetteur.
- Sur le serveur: *messageDate* est égal à la date actuelle moins 23 jours ➔ code de statut «701 Message expires soon» à l'adaptateur émetteur.
- Sur le serveur: *messageDate* est égal à la date actuelle moins 30 jours ➔ code de statut "204 message expired" à l'adaptateur émetteur.

Le code de statut "701" a valeur d'avertissement pour l'émetteur, à qui il donne la possibilité d'intervenir le cas échéant auprès du destinataire, pour que celui-ci réceptionne le message ou vérifie le fonctionnement de son adaptateur.

Si après l'envoi, l'émetteur reçoit le code de statut "204" (au lieu de "100"), le message ne peut plus être téléchargé par le récepteur. Le cas échéant, on relancera la procédure dans l'application participante.

3.10 Exemples

Ce chapitre donne des exemples d'enveloppes et de quittances sedex, sur la base de cas d'utilisation concrets. Pour des raisons de place, il a été renoncé dans ces exemples à mentionner les références aux fichiers du schéma XML (xsi:schemaLocation).

3.10.1 Exemple: livraison de la commune d'Olten à la statistique

Dans l'exemple suivant, la commune d'Olten (sedex ID: 1-2581-1) livre le 21.01.2011 avec un jour de référence fixé au 31.12.2010 ses données à l'OFS (sedex ID: 3-CH-1).

Message 1 : Livraison de l'ensemble des données d'Olten à l'OFS (eventDate désigne le jour de référence de la livraison ; messageDate désigne le moment de l'élaboration du message à destination de l'OFS):

```
<?xml version="1.0" encoding="UTF-8"?>
<envelope xmlns="http://www.ech.ch/xmlns/eCH-0090/1"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  version="1.0">
  <messageId>550e8400-e29b-11d4-a716-446655440000</messageId>
  <messageType>99</messageType>
  <messageClass>0</messageClass>
  <senderId>1-2581-1</senderId>
  <recipientId>3-CH-1</recipientId>
  <eventDate>2010-12-31T00:00:00</eventDate>
  <messageDate>2011-01-21T12:34:56</messageDate>
</envelope>
```

Quittance par rapport au message 1 (générée par l'adaptateur sedex de la commune d'Olten; eventDate désigne le moment de la livraison du message à l'OFS):

```
<?xml version="1.0" encoding="UTF-8"?>
<receipt xmlns="http://www.ech.ch/xmlns/eCH-0090/1"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  version="1.0">
  <eventDate>2011-01-21T12:45:00Z</eventDate>
  <statusCode>100</statusCode>
  <statusInfo>Message correct transmitted</statusInfo>
  <messageId>550e8400-e29b-11d4-a716-446655440000</messageId>
  <messageType>99</messageType>
  <messageClass>0</messageClass>
  <senderId>1-2581-1</senderId>
  <recipientId>3-CH-1</recipientId>
</receipt>
```

Message 2 : quittance spécifique de l'OFS à la commune d'Olten :

```
<?xml version="1.0" encoding="UTF-8"?>
<envelope xmlns="http://www.ech.ch/xmlns/eCH-0090/1"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  version="1.0">
  <messageId>13</messageId>
  <messageType>99</messageType>
  <messageClass>2</messageClass>
  <referenceMessageId>550e8400-e29b-11d4-a716-446655440000</referenceMessageId>
  <senderId>3-CH-1</senderId>
  <recipientId>1-2581-1</recipientId>
  <eventDate>2010-12-31T00:00:00</eventDate>
  <messageDate>2011-01-21T13:00:00</messageDate>
</envelope>
```

Quittance par rapport au message 2 (générée par l'adaptateur de l'OFS) :

```
<?xml version="1.0" encoding="UTF-8"?>
<receipt xmlns="http://www.ech.ch/xmlns/eCH-0090/1"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  version="1.0">
  <eventDate>2011-01-21T13:15:00Z</eventDate>
  <statusCode>100</statusCode>
  <statusInfo>Message correct transmitted</statusInfo>
  <messageId>13</messageId>
  <messageType>99</messageType>
  <messageClass>2</messageClass>
  <senderId>3-CH-1</senderId>
  <recipientId>1-2581-1</recipientId>
</receipt>
```

Message 3 : réponse de l'OFS à la commune d'Olten :

```
<?xml version="1.0" encoding="UTF-8"?>
<envelope xmlns="http://www.ech.ch/xmlns/eCH-0090/1"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  version="1.0">
  <messageId>48</messageId>
  <messageType>99</messageType>
  <messageClass>1</messageClass>
  <referenceMessageId>550e8400-e29b-11d4-a716-446655440000</referenceMessageId>
  <senderId>3-CH-1</senderId>
  <recipientId>1-2581-1</recipientId>
  <eventDate>2010-12-31T00:00:00</eventDate>
  <messageDate>2011-01-22T06:00:00</messageDate>
</envelope>
```

Quittance par rapport au message 3 (générée par l'adaptateur de l'OFS) :

```
<?xml version="1.0" encoding="UTF-8"?>
<receipt xmlns="http://www.ech.ch/xmlns/eCH-0090/1"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  version="1.0">
  <eventDate>2011-01-22T14:13:02Z</eventDate>
  <statusCode>100</statusCode>
  <statusInfo>Message correct transmitted</statusInfo>
  <messageId>48</messageId>
  <messageType>99</messageType>
  <messageClass>1</messageClass>
  <senderId>3-CH-1</senderId>
  <recipientId>1-2581-1</recipientId>
</receipt>
```

Le diagramme de séquence suivant illustre le scénario de livraison présenté ci-dessus.

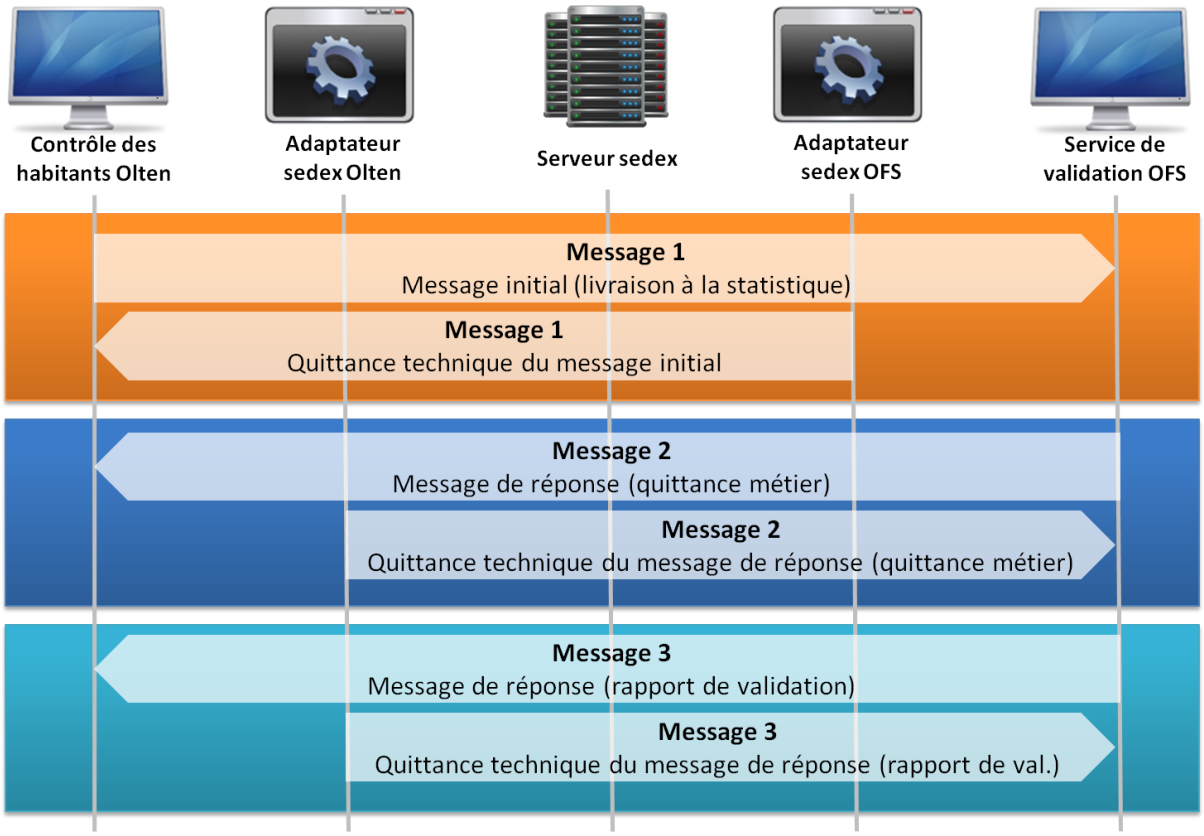


Illustration 12: Echange de données entre le contrôle des habitants de la ville de Olten et l'OFS

3.11 Proxy service web

3.11.1 But du Proxy service web

Les applications participantes peuvent utiliser des services web sans avoir elles-mêmes à s'authentifier de manière explicite vis-à-vis du prestataire de service ou à effectuer le cryptage des données. L'authentification et le cryptage sont effectués automatiquement par sedex au moyen du certificat d'organisation de l'adaptateur. A cet effet, sedex propose un Proxy service web qui réplique chez le client les points finaux correspondants du fournisseur de prestations.

3.11.2 Fonctionnement du Proxy service web

Le Proxy service web réceptionne les appels service web destinées à certains points finaux, les authentifie, les crypte et les dirige vers le point final du fournisseur de prestations correspondant. Les réponses des fournisseurs de prestations sont, si nécessaire, authentifiées et décryptées par le Proxy service web et retransmises à l'émetteur d'origine. L'illustration 13 illustre ce processus.

3.11.3 Echange de messages

L'échange de message qui a lieu via le Proxy service web s'effectue de manière synchrone contrairement à l'adaptateur, qui lui, permet d'échanger des messages de manière asynchrone.

Le Proxy service web n'apporte aucune modification au message adressé à l'un de ses points finaux, à l'exception du cryptage/de la signature; en d'autres termes, le contenu des messages est retransmis tel quel au fournisseur de prestations. La même règle s'applique à la réponse renvoyée par ce dernier.

Le Proxy service web ne procède à aucune autorisation. Seul le fournisseur de prestation y est habilité. Toutefois, le Proxy service web ne supporte que les services qui reconnaissent le certificat d'organisation de l'adaptateur sedex comme un certificat d'autorisation.

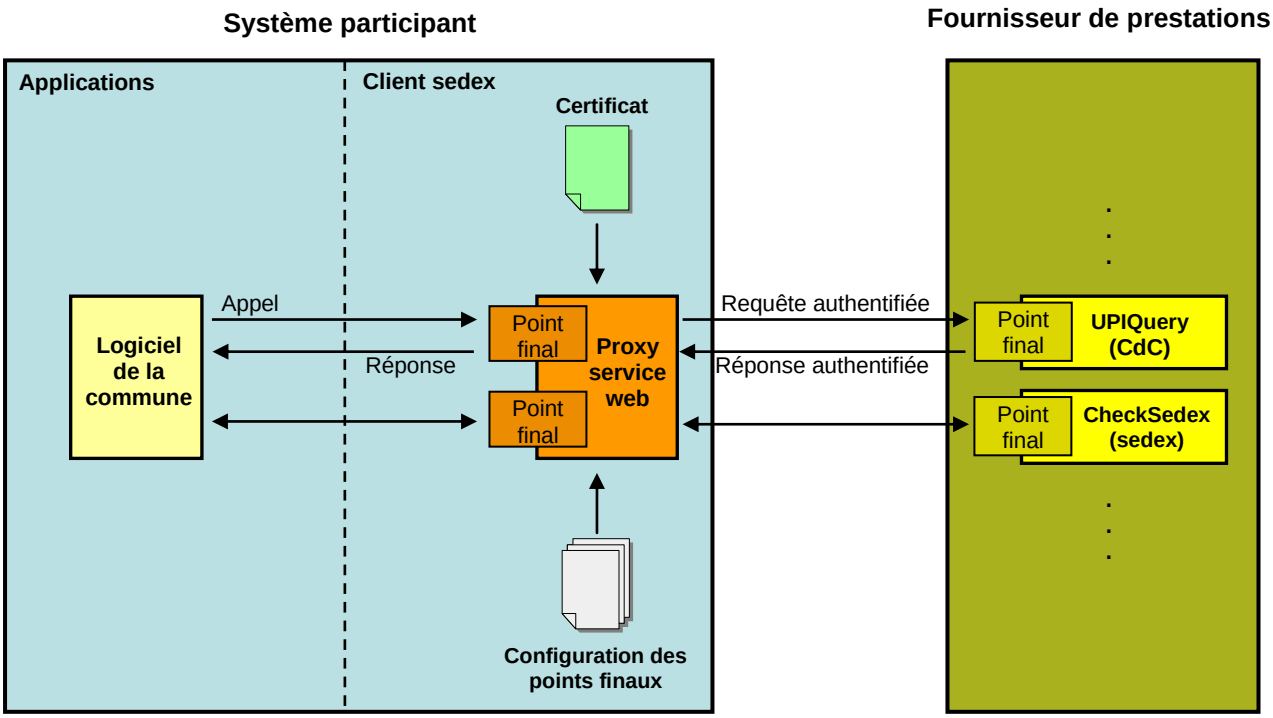


Illustration 13: Proxy service web

3.11.4 Accès au Proxy service web

Le proxy service web n'identifie pas l'appelant à l'aide de l'ID sedex. L'appel peut donc en principe être effectué depuis n'importe quel ordinateur pouvant atteindre le proxy service web. Il est du ressort de l'exploitant de ce dernier de s'assurer que, seuls les acteurs autorisés à utiliser des services web, puissent atteindre le proxy service web.

Les capacités du serveur sur lequel est installé le proxy service web et l'adaptateur sedex pourraient être insuffisantes en fonction du nombre et de la taille des appels de services. Si une grande charge est envisagée, il est conseillé de prévoir un serveur dédié au proxy service web.

3.11.5 Services web compatibles

Les services web suivants acceptent l'authentification au moyen du certificat d'organisation:

Webservice	Documentation
CheckSedex	cf. chapitre 8.3
UPIQueryService	cf. [8]
UPICompareService	cf. [8]

Le Proxy service web sedex ne propose en principe que des services qui peuvent être directement appelés en utilisant le certificat du participant sedex. La configuration du proxy définit quels points finaux sont répliqués localement auprès de l'utilisateur et de quelle manière les requêtes sont transmises au prestataire de service.

3.12 Aspects de l'exploitation de l'adaptateur sedex

3.12.1 Délais de conservation

Il n'y a pas de délai de conservation pour les messages et les quittances reçues ou envoyées par l'adaptateur sedex.

Lorsqu'il existe des règles de conservation des données transmises par sedex, celles-ci doivent être conservées par l'application participante.

L'adaptateur n'efface ni les messages (dossiers *inbox, outbox* et *sent*), ni les quittances techniques (dossier *receipts*). Il revient à l'application participante de supprimer ces données, selon des règles utiles (p. ex. périodiquement sur la base de l'âge ou à la clôture d'un cas).

Les fichiers log sont écrasés dès que le nombre maximal de fichiers log est atteint (principe du rollover). Cette mesure n'affecte pas la journalisation établie par le serveur sedex.

3.12.2 Version du schéma XML eCH-0090

Les enveloppes et les quittances techniques sont construites sur la base du schéma XML eCH-0090. L'application participante devrait être en mesure de traiter des enveloppes créées à partir de différentes versions de schémas XML. A noter que lors de Major Releases (2.0, 3.0,…), les espaces de noms de l'URL change. Exemple : «*xmlns :eCH-0090=http://www.eCH.ch/eCH-0090/**2***» pour le schéma eCH-0090, version **2.0**.

L'OFS fixera toutefois des délais limitant l'utilisation de l'ancienne version du schéma.

Si, lors de l'apparition de nouveaux codes de statut, les éventuelles modifications à effectuer sur l'application participante doivent être repoussées, il est possible d'indiquer dans la configuration de l'adaptateur, selon quelle version du schéma XML la quittance doit être créé.

Les enveloppes (/eCH-0090:envelope) doivent toujours être construites suivant la version 1.0 du schéma XML eCH-0090, alors que les quittances sont par défaut générées selon la version 2.0 du schéma XML eCH-0090.

3.13 Messages de service sedex

L'OFS, en tant qu'exploitant de la plateforme sedex, a la possibilité de pouvoir communiquer avec l'adaptateur lui-même. Le champ d'action des messages de service sedex sont :

- Le renouvellement automatique des certificats d'organisation (voir chapitre 4.6)
- Le renouvellement automatique du truststore du proxy service web

Les messages de service sont livrés dans un répertoire différent. Ces messages sont par la suite pris en charge par l'adaptateur lui-même. Les autorisations permettant la réception des messages sont effectuées de manière indépendante au niveau de l'administration du système sedex.

Le traitement correct des messages de service est surveillé par l'administration sedex qui, en cas de problème et si un traitement manuel est nécessaire, prends contact avec le participant.

3.14 Polling

Le client sedex se connecte régulièrement au serveur sedex pour vérifier la présence de nouveaux messages dans la boîte aux lettres du serveur. L'intervalle de balayage (polling) définit la période entre deux connexions. Par défaut, l'intervalle de polling est défini comme suit:

Période	Intervalle de balayage
07h00 – 18h59	5 minutes
19h00 – 06h59	15 minutes

Note: L'intervalle de balayage a été choisi de manière à convenir à tous les utilisateurs et optimiser la performance du serveur sedex et il ne devrait donc pas être modifié. Veuillez prendre contact avec le service clientèle (voir chapitre 5.1) s'il est malgré tout nécessaire de modifier l'intervalle de balayage.

3.15 Surveillance des composants

A partir de la version 4.0, il est possible de surveiller le bon fonctionnement du client sedex.

Les informations suivantes sont à disposition:

- Version de l'adaptateur
- Version du proxy service web
- Version du controller
- sedex ID de l'installation
- Profil de l'adaptateur (voir chapitre 3.16)
- Date d'expiration du certificat d'organisation
- Date d'expiration du certificat de mise à jour
- Présence des dossiers d'interface
- Connectivité avec le serveur sedex
- Version de chaque archive AAR
- Version du truststore du proxy service web
- Durée de fonctionnement de l'adaptateur
- Durée de fonctionnement du proxy service web
- Durée de fonctionnement du controller

Il existe deux possibilités pour obtenir l'état du client sedex:

- Fichier monitoring
- Appel HTTP

3.15.1 Fichier monitoring

Le fichier monitoring est généré à intervalle de 5 minutes par le controller sedex. Le fichier est au format texte (text/plain) et comporte les informations listées ci-dessus. Le fichier monitoring.txt se trouve dans le répertoire monitoring.

Par défaut, la génération du fichier monitoring est activée. Il est possible de désactiver le monitoring, mais aussi de définir l'emplacement du fichier et l'intervalle de vérification à l'aide des paramètres adéquats dans le fichier de configuration du client sedex (voir document [7]).

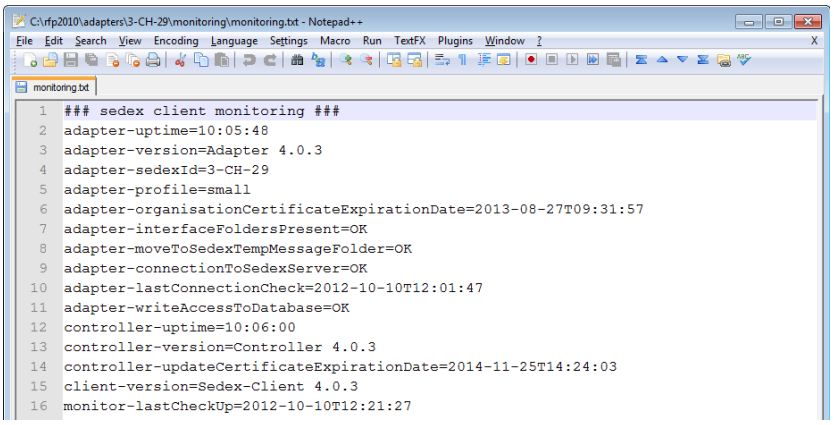


Illustration 14: Aperçu du fichier monitoring

3.15.2 Requête HTTP

La requête HTTP permet de se connecter au service HTTP mis à disposition par le controller sedex sur le port 8000. La réponse est au format texte (text/plain) et comporte les informations listées ci-dessus. Pour utiliser la requête HTTP, il faut utiliser l'URL suivante: http://[hote]:[port]/monitoring (p.ex. http://localhost:8000/monitoring).

Par défaut, le serveur HTTP du monitoring est activé. Il est possible de désactiver le monitoring, mais aussi de définir le port et l'intervalle de vérification à l'aide des paramètres adéquats dans le fichier de configuration du client sedex (voir document [7]).

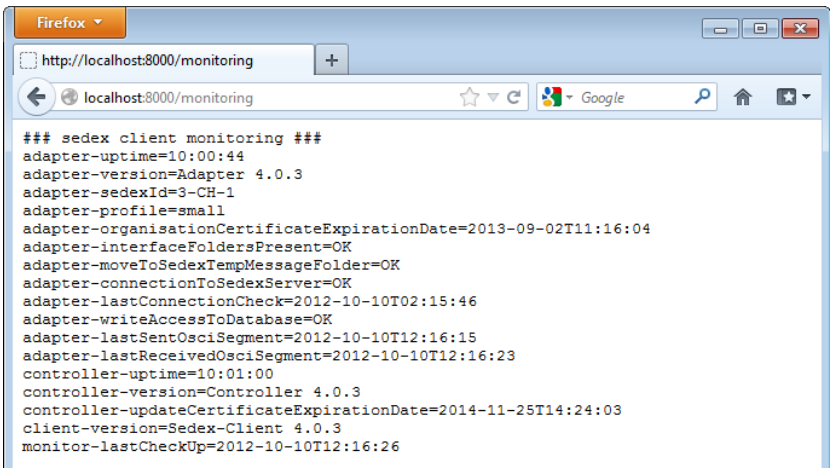


Illustration 15: Aperçu de la réponse à la requête HTTP

3.16 Optimisation du client sedex

Le client sedex est prévu pour être utilisé sur toutes sortes de plateformes, allant de l'ordinateur de bureau d'entrée de gamme au serveur haute performance. Pour profiter au mieux des capacités de la machine sur laquelle le client doit être installé, il est possible de choisir parmi quatre profils définissant notamment le nombre de processus parallèles et le nombre de connexions simultanées vers le serveur sedex.

Le choix du profil influence grandement la performance de l'adaptateur sedex. Cependant, la puissance peut aussi être augmentée en adaptant la limite maximale de la mémoire vive (RAM) utilisable par la machine virtuelle Java.

Le profil doit être choisi en fonction de l'environnement de l'adaptateur:

- caractéristiques machine (CPU, mémoire, place disque)
- réseau (débit du réseau interne/Internet, présence de pare-feu, etc.)

Le tableau suivant résume les caractéristiques des différents profils:

	small *	**medium**	**large**	**x-large**
Connexions au serveur sedex	1x	2x	4x	8x
Processus parallèles (threads)	2x	3x	5x	7x
Scripts de nettoyage (cleaning job)	15 min.	30 min.	45 min.	60 min.

* Profil par défaut

Plus de renseignements au sujet des possibilités d'optimisation dans le document [7]. Le service clientèle de l'OFS (chapitre 5.1) se tient également à disposition pour plus d'informations au sujet du changement de profil.

3.17 Verrouillage des applications

Dans l'optique d'offrir une plus grande fiabilité, le verrouillage des applications, qui empêche le démarrage multiple d'une même instance, a été amélioré de façon à ne plus empêcher le démarrage après un arrêt brutal. Le controller et le proxy service web sont également équipés de ce nouveau verrouillage.

3.18 Assistance à distance

3.18.1 Mécanisme des commandes

Dès la version 4.0, le client intègre un mécanisme de commandes à distance qui permet à l'administration sedex d'effectuer certaines actions précises et clairement délimitées sur le client sedex dans le but d'assister les utilisateurs et les exploitants du client sedex.

Il ne s'agit en aucun cas d'un accès à distance (RDP, SSH, Telnet, VNC, etc.), mais d'un ensemble de cinq commandes que l'administration sedex peut, le cas échéant, déposer auprès de clients sedex.

Seul l'administration sedex peut saisir ces commandes. Les utilisateurs et exploitants du client sedex n'ont pas la possibilité d'utiliser cette fonctionnalité.

Le tableau suivant dresse une liste exhaustive des commandes disponibles:

Commande	Description
getconfig	Récupération de tous les fichiers de configuration du client sedex
getlogs	Récupération des tous les fichiers logs du client sedex
start	Démarrage de l'adaptateur sedex et/ou du proxy service web sedex
stop	Arrêt de l'adaptateur sedex et/ou du proxy service web sedex
update	Mise à jour du client sedex

3.18.2 Récupération de la configuration et des logs

La récupération de la configuration et des logs est lancée via une commande *getconfig* ou *getlogs*.

Pour préserver la sécurité proposée par sedex, le certificat n'est pas transmis et les mots de passe présent dans les fichiers de configuration sont masqués.

3.18.3 Mise à jour

La mise à jour est lancée via une commande update.

Pour plus de sécurité, les paquets de mise à jour sont signés numériquement, ce qui empêche l'installation de logiciels tiers malveillant.

Par défaut, le mécanisme de mise à jour est activé (désactivé dans la version 4.0.3). Cette valeur peut être modifiée à l'aide d'un paramètre adéquat dans le fichier de configuration du client sedex (voir document [7]).

Rappel: Les mises à jour (comme tout autre type de commande) sont téléchargées et appliquées uniquement auprès des participants défini par l'administration sedex dans la commande.

3.19 Journalisation

Durant son fonctionnement, le client sedex génère des fichiers logs qui permettent, en cas de problèmes, d'analyser les erreurs rencontrées.

Chaque composant du client sedex (controller, adaptateur et proxy service web) génère au minimum un fichier log.

Le chapitre 8.5 décrit en détail les différents logs et leur contenu.

4 Processus

4.1 Vue d'ensemble

Le raccordement d'une application et/ou d'un participant à sedex peut être subdivisé en trois phases, à savoir le développement, l'introduction et l'exploitation.

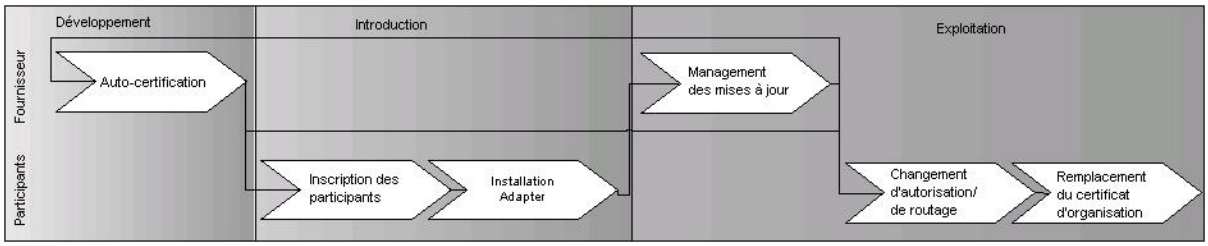


Illustration 16: Chaîne de processus sedex

4.2 Certification des applications participantes

Le coordinateur du domaine spécialisé peut exiger la certification de l'application avant le raccordement du premier participant.

Il revient au coordinateur de déterminer la forme et l'objet de la certification, qui figurent dans la documentation établie pour le raccordement de l'application à sedex.

Pour le domaine de l'harmonisation des registres, la section SR de l'OFS a opté pour l'auto-certification, dont l'objet est décrit sous [4].

Chaque coordinateur peut décider s'il veut exiger une certification ou une auto-certification pour son domaine.

4.3 Annonce d'un participant

La participation à sedex est conditionnée à la certification, par le fournisseur, de l'application participante à sedex (voir chapitre 4.2).

4.3.1 Préparer l'annonce

Le futur participant et son fournisseur de logiciels collectent les informations nécessaires à l'annonce:

- Nom et adresse e-mail du participant
- Nature et nom de l'application avec laquelle les messages sedex seront établis (p. ex. registre de l'état civil, Infostar)
- Type de raccordement à sedex (direct ou indirect, cf. chapitre 2.4)
- En cas de raccordement indirect: nom du récepteur par défaut
- En cas de raccordement direct: adresse postale pour la livraison du certificat d'organisation
- Délai pour le raccordement
- Nom et adresse e-mail de la personnes chargée du raccordement.

4.3.2 Annoncer les participants à l'OFS

Le futur participant ou son fournisseur de logiciels annonce le ou les nouveaux participant(s) via le coordinateur du domaine métier au service clientèle de l'OFS:

Cette annonce peut s'effectuer par téléphone ou par e-mail:

- Téléphone: 0800 866 700
- E-mail harm@bfs.admin.ch

L'annonce doit avoir lieu au plus tard deux semaines avant la date de raccordement souhaitée. Au-delà, il n'est pas garanti que le raccordement puisse être effectué à la date souhaitée.

4.4 Installation du client sedex

Les explications suivantes ne concernent que les participants raccordés directement à sedex.

Le client sedex est un terme qui regroupe le controller sedex, l'adaptateur sedex et le proxy service web.

4.4.1 Exigences en matière de configuration réseau

4.4.1.1 Serveur Proxy

Si les exigences ou besoins locaux exigent l'utilisation d'un serveur proxy, les paramètres correspondants doivent être renseignés dans les fichiers de configuration des différents composants du client sedex.

4.4.1.2 Routeur

Si les autorités communales ou locales le souhaitent, le flux de données adaptateur-serveur peut transiter par le réseau cantonal et/ou fédéral (KOMBV/KTV).

Cependant, il faut noter que les caractéristiques de sécurité de sedex permettent une communication via Internet sans risque.

4.4.1.3 Pare-feu

Le pare-feu doit être configuré de telle sorte à autoriser les communications sortantes pour les ports 80 (HTTP) et 443 (HTTPS). En tant que configuration minimale, il s'agirait d'autoriser l'application « java.exe » pour ces deux ports.

Etant donné que le client sedex ne fait jamais office de serveur, les ports ne doivent pas être ouverts pour les données entrantes.

4.4.2 Préparation de la configuration réseau

4.4.2.1 Vérification de la connectivité au serveur sedex

Avec les anciennes versions, toutes les communications nécessaires entre l'adaptateur sedex et le serveur transitaient via SOAP-over-OSCI. Du point de vue de l'adaptateur, seule l'adresse du serveur OSCI (www.governikus.admin.ch) devait donc être accessible.

L'introduction de SOAP-over-HTTPS signifie concrètement que l'adaptateur (≥ v2.2) doit pouvoir accéder aux adresses suivantes:

- www.governikus.admin.ch (port 80)
- www.oscitv-gw.admin.ch (port 443)
- www.sedex-gw.admin.ch (port 443)
- www.osciservices-gw.admin.ch (port 443)

La connectivité pour l'adresse *www.governikus.admin.ch* peut être vérifiée facilement à l'aide d'un navigateur. Pour cela, indiquez dans le navigateur web de la machine sur laquelle vous désirez installer le client sedex l'adresse suivante:

http://www.governikus.admin.ch/osci-manager-entry/externalentry

Si le message suivant s'affiche, le module Governikus du serveur sedex est atteignable:

I don't speak GET – Send POST to URL - -

Il n'est malheureusement pas possible de vérifier si les adresses *www.oscitv-gw.admin.ch*, *www.sedex-gw.admin.ch* et *www.osciservices-gw.admin.ch* sont atteignable à l'aide d'un navigateur web. Les composants réseaux (comme proxy, serveur DNS, routeur, pare-feu) des participants sedex doivent donc être configurés en conséquence si des problèmes de connexion sont constatés.

La version 4.0 du client sedex effectue une vérification des URL au démarrage de l'adaptateur sedex. Le résultat de la vérification est visible dans le log technique de l'adaptateur sedex ou dans le monitoring.

Extrait du log technique de l'adaptateur:

```
...
Connection test for <https://www.sedex-gw.admin.ch/sedex-runtime-ws/SedexAuthorisationImpl?WSDL>: passed
Connection test for <http://www.governikus.admin.ch/osci-manager-entry/externalentry>: passed
Connection test for <https://www.osciservices-gw.admin.ch/pros-logic/iProSLogic?WSDL>: passed
Connection test for <https://www.oscitv-gw.admin.ch/idm-services/idm_iGet/V1?WSDL>: passed
Connection test finished successfully
...
```

Extrait du monitoring:

```
...
adapter-connectionToSedexServer=OK
adapter-lastConnectionCheck=2012-10-18T15:13:59
...
```

Pour plus de détails, veuillez vous référer au document [7].

4.4.2.2 Vérification de la connectivité aux prestataires de services web

Dans le cadre de sont fonctionnement, le proxy service web doit pouvoir accéder au services web des différents prestataires de service.

UPI Services

Les adresses suivantes sont nécessaire au proxy service web pour permettre l'interrogation du service UPI :

- https://wupi.zas.admin.ch/wupi_cc/UPIQueryService
- https://wupi.zas.admin.ch/wupic_cc/UPICompareService

CheckSedex

L'adresse suivante est nécessaire au proxy service web pour permettre l'interrogation du service CheckSedex :

- https://www.sedex-gw.admin.ch/sedex-runtime-ws/CheckSedexWebService

4.4.2.3 Détermination du serveur Proxy

Si le flux de données entre le client sedex et le serveur sedex doit transiter par un proxy, les informations suivantes sont nécessaires :

- URL du serveur Proxy (p.ex. myhost.at.com)
- Port, sur lequel le serveur Proxy peut être atteint (p.ex. 8080 ou 8088)

Par la même occasion, il est souhaitable de savoir si l'accès à ce proxy est ouvert ou si un login est nécessaire. Dans le dernier cas, les informations suivants vous seront utiles :

- Nom d'utilisateur
- Mot de passe

Ces données, qui doivent être introduites dans les fichiers de configuration suivants, peuvent être obtenues auprès du responsable de votre réseau informatique :

- adapter/conf/sedexAdapter.properties
- adapter/conf/wsproxy.properties
- controller/conf/sedexController.properties

L'URL et le port peuvent également être découverts par soi-même :

- Démarrez votre navigateur (p.ex. Windows Internet Explorer, Firefox). La description suivante se réfère à Internet Explorer 8.0.
- Choisissez Outils – Options Internet – Connexions – Paramètres réseau
- Contrôlez les données de la fenêtre ci-dessous :

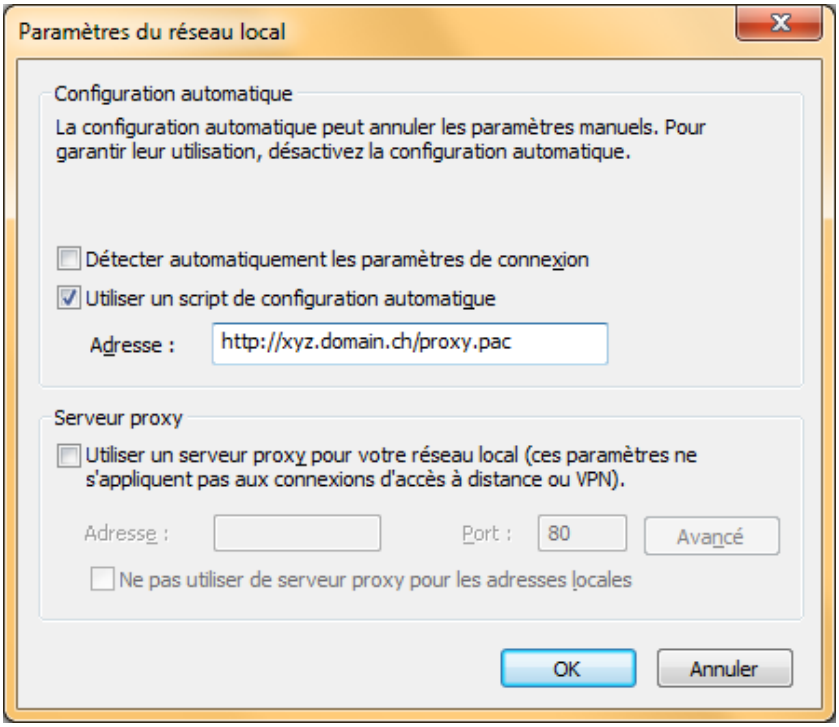

Paramètres du réseau local
Configuration automatique
La configuration automatique peut annuler les paramètres manuels. Pour garantir leur utilisation, désactivez la configuration automatique.
Détecter automatiquement les paramètres de connexion
Utiliser un script de configuration automatique
Adresse :
http://xyz.domain.ch/proxy.pac
Serveur proxy
Utiliser un serveur proxy pour votre réseau local (ces paramètres ne s'appliquent pas aux connexions d'accès à distance ou VPN).
Adresse :
Port :
80
Avancé
Ne pas utiliser de serveur proxy pour les adresses locales
OK
Annuler

Illustration 17: Configuration du proxy sur Internet Explorer 8.0

- Si la case à cocher sous la rubrique « Serveur proxy » est activée, les données se trouvant dans cette même rubrique sont à observer et à saisir dans les différents fichiers de configuration du client sedex.
- Si la case à cocher « Utiliser un script de configuration automatique » est activée, éditez le fichier indiqué (p.ex. avec WordPad) et vérifiez quel règles sont définies pour les adresses nécessaires au client sedex (voir chapitre 4.4.2.5).
- Si aucune case à cocher n'est active, la connexion a lieu directement, sans transiter par un proxy.

4.4.2.4 Définition du routage

Renseignez-vous auprès des responsables du réseau informatique communal et/ou cantonal quant au canal à utiliser pour les données sedex :

- Le serveur sedex peut-il être atteint par Internet ?
- Le serveur sedex doit-il être atteint via un proxy (cantonal) ?
- Le serveur sedex doit-il être atteint via le réseau KOMBV/KTV ?

4.4.2.5 Vérification de la configuration réseau

Afin de vérifier si des changements sont à effectuer dans votre configuration réseau en fonction de la décision prise au chapitre 4.4.2.4, on peut demander au système de fournir l'adresse IP du serveur sedex sur la base de l'URL :

- Démarrer la console de commande
- Entrer la commande nslookup www.governikus.admin.ch

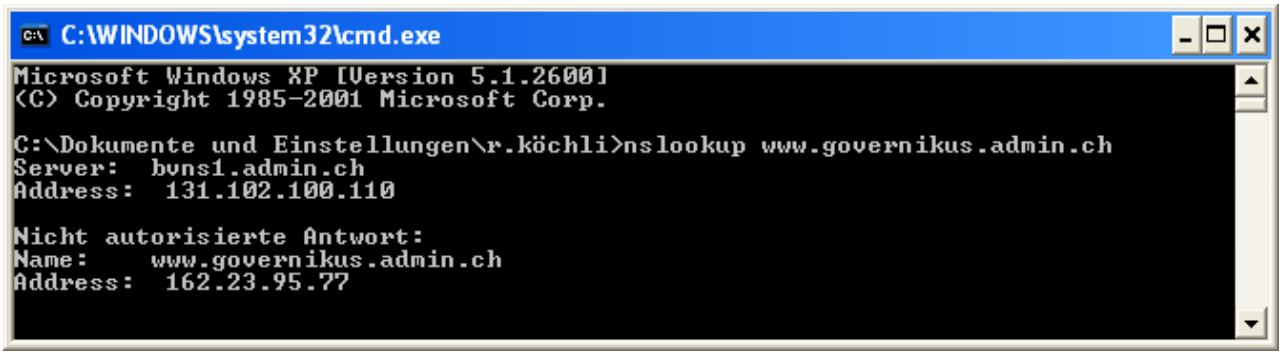


Illustration 18: Exemple de ligne de commande MS-DOS (Windows), lorsque l'on passe par le réseau KOMBV

Illustration 19: Exemple de ligne de commande Bash (Linux), lorsque l'on passe par Internet

Sous Linux, la commande peut être exécutée en tant qu'utilisateur normal.

Grâce à la réponse, le chemin utilisé pour atteindre le serveur peut être déterminé :

- Adresse IP 162.23.95.77: Connexion via le réseau KOMBV
- Adresse IP 162.23.40.61: Connexion via Internet.

Le cas échéant, des modifications devront être apportées au serveur DNS (voir chapitre 4.4.2.6).

4.4.2.6 Organiser la configuration du serveur DNS

Si le serveur sedex ne doit pas être atteint directement (par Internet), mais à travers un réseau cantonal et/ou inter-cantonal (KOMBV/KTV), il est nécessaire de mandater les personnes responsables du réseau correspondant dans le but d'effectuer le routage correct.

A cette fin, les indications suivantes doivent être fournies :

- Adresse IP d'où une connexion sera établie avec le serveur sedex (machine où le client sedex est installé). Si un proxy est utilisé, c'est l'adresse du proxy qui est pertinente.
- Adresse IP du serveur sedex. Cette indication est dépendante du choix de connexion et des résultats obtenus au chapitre 4.4.2.5. L'URL du serveur sedex doit pouvoir être résolue conformément au choix de connexion.

On effectuera la même opération pour tous les serveurs et pour tous les prestataires de services à atteindre par l'intermédiaire du client sedex.

4.4.2.7 Ouverture des ports

Clarifiez avec les responsables de votre réseau informatique si les ports 80 (HTTP) et 443 (HTTPS) sont ouverts pour les connexions sortantes (voir chapitre 4.4.1.3).

4.4.3 Installation

Un client sedex doit être installé par participant direct (physique). La partie responsable de cette installation est l'organisation supportant le participant pour les questions informatiques.

L'installation de l'adaptateur se déroule de préférence en même temps que l'installation de la version certifiée de l'application participante.

4.4.3.1 Configuration requise

La configuration requise faisant foi est décrite dans le manuel d'installation du client sedex (voir document [7]) qui se trouve également sur le site Internet de l'OFS. Les paragraphes ci-dessous soulignent les points les plus importants.

Pour des performances optimales, nous recommandons l'utilisation d'une machine équipée de processeur "Dual-Core" ayant un minimum de 512 Mo de mémoire vive (RAM) dédiée aux composants du client sedex. Le client sedex nécessite la version 1.6 de java (mise à jour 1 à 43).

Il est en outre possible de choisir parmi plusieurs profils d'utilisation. Les exigences minimales peuvent donc changer selon le profil choisi. Plus d'informations au sujet des profils au chapitre 3.16.

4.4.3.2 Privilèges

Durant son exploitation, le client sedex doit pouvoir accéder, lire et écrire des fichiers à différents emplacements de l'installation sedex. Le dossier du client sedex, mais aussi tous ses sous-dossiers doivent donc être accessibles sans limitation par le client sedex. En revanche, le client ne nécessite aucun accès en dehors de son arborescence.

Sur les systèmes Windows, il faut définir le privilège «contrôle total», alors que sur les systèmes de type Unix/Linux, il faut définir le droit «rwx». L'adaptateur sedex ne nécessite pas de droit d'écriture sur d'autres dossiers du système.

Si le client sedex est démarré en tant qu'application (script bin/controller-start.bat ou bin/controller-start.sh), les droits ci-dessus doivent être définis pour l'utilisateur qui utilisera le

client. Si le client est démarré en tant que service Windows ou daemon Unix/Linux, ces mêmes droits doivent être appliqués à l'utilisateur «System» (Windows) ou «root» (Unix/Linux).

4.5 Modification des autorisations / routage

Les demandes de modification des types de messages autorisés et/ou des règles de routage doivent être adressées par les participants mêmes ou par les fournisseurs au Service clientèle de l'OFS (chapitre 5.1).

4.5.1 Modification des autorisations

Seuls doivent être annoncés les types de messages que le participant souhaite voir ajouter à ceux ou retirés de ceux qui ont été inclus dans l'auto-certification par son fournisseur de logiciel.

Il n'est pas nécessaire que chaque participant procède à une requête isolée pour demander l'ajout, par le fournisseur, de types de messages supplémentaires lors du renouvellement de l'auto-certification; le service clientèle de l'OFS veille à ce que les clients du fournisseur qui sont déjà autorisés le soient également pour les nouveaux types de message. Selon le nombre des participants concernés, le service clientèle conviendra avec le fournisseur du délai dans lequel les mutations doivent s'effectuer.

4.5.2 Modification du routage

Les participants qui souhaitent passer à un raccordement indirect à sedex doivent désigner le nom du récepteur par défaut. Sauf instruction contraire, le certificat d'organisation est révoqué après le changement de routage.

Les participants qui souhaitent passer à un raccordement direct à sedex doivent annoncer l’adresse postale pour la livraison du certificat d’organisation.

4.6 Renouvellement du certificat d'organisation

4.6.1 Types de renouvellement

Les certificats d'organisation sont valables trois ans. En principe, le renouvellement s’effectue **automatiquement** (voir chapitre 4.6.2).

Si le participant est une instance de test (p.ex. T3-CH-1), le renouvellement doit être **effectué manuellement** (voir chapitre 4.6.3).

En raison des désavantages que représente le renouvellement manuel (voir chapitre 8.4.3), l’OFS recommande d’utiliser le renouvellement automatique du certificat.

4.6.2 Renouvellement automatique

L’adaptateur déclenche de lui-même le renouvellement entre 60 et 90 jours avant la date d’expiration. Pour des raisons de planification, les administrateurs sedex (c-à-d l’OFS) ont également la possibilité de déclencher le renouvellement.

Le processus de renouvellement automatique est décrit dans le chapitre 8.4.2. La seule intervention manuelle consiste pour les administrateurs sedex à confirmer le renouvellement.

L’OFS surveille l’installation correcte du nouveau certificat et contacte, le cas échéant, le participant (il peut également s'agir du fournisseur ou de l'exploitant).

4.6.3 Renouvellement manuel

Le renouvellement manuel correspond fondamentalement au processus de première installation du certificat d'organisation (8.4.1).

Le nouveau certificat doit être sollicité auprès du service clientèle (voir chapitre 5.1). Par défaut, l'OFS livre le certificat et le mot de passe au participant. Si le certificat doit être livré à un fournisseur ou un exploitant, il est nécessaire d'indiquer l'adresse email de livraison lors de la commande.

Le participant est responsable de l'installation du certificat. L'installation manuelle nécessite un redémarrage de l'adaptateur, une fois le renouvellement terminé.

La période entre la commande du nouveau certificat auprès du service clientèle et l'installation doit être aussi courte que possible, afin d'éviter des problèmes de cryptage liés à la transition de l'ancien vers le nouveau certificat.

L'OFS recommande donc de réserver suffisamment de temps pour effectuer en une fois la commande et l'installation du nouveau certificat.

4.7 Management des mises à jour

Le développement ultérieur de la plateforme sedex et les modifications de l'adaptateur sedex qui y seront liées se dérouleront selon des étapes bien définies. Il faut s'attendre à deux mises à jour par an au maximum.

L'OFS annonce dans ses Release Notes les modifications et les innovations accompagnant la nouvelle version du client. Les Release Notes sont publiées avec le présent manuel.

Le présent manuel et le guide d'installation sont mis à jour lors de chaque publication d'une nouvelle version du client.

La compatibilité des nouvelles versions avec les versions antérieures est assurée au moins jusqu'à la version n.0 de la version courante. A titre d'exemple, la version 4.9 est compatible avec la 4.0, mais pas avec la 3.9. La compatibilité des différentes versions d'adaptateur est décrite dans les Release Notes.

Nous recommandons cependant l'installation de la dernière version du client sedex, lorsque l'application participante est mise à jour.

Le client sedex peut être téléchargé depuis le site Internet de l'OFS[9]. Ce site internet[10] renseigne également au sujet des prochaines mises à jour prévues. La liste des mises à jours contient notamment la planification de publication des composantes informatiques, des nomenclatures, et des règles de validation, etc...

[9] http://www.sedex.ch > Clients sedex et documentation
[10] http://www.registre-stat.admin.ch > Spécifications informatiques > Release Management

4.7.1 Support des différentes versions

La fin du support s'effectue en deux étapes. Le support complet s'arrête en principe 18 mois après la publication. Passée cette date, un support réduit est mis à disposition: En cas de disfonctionnement une recherche est effectuée mais le problème n'est pas transmis pour résolution à l'office fédéral de l'informatique (OFIT). Ce support réduit se termine en général 24 mois après la publication. Plus aucun support n'est mis à disposition au-delà de la fin du support réduit.

Version du client	Publication	Fin du support complet	Fin du support réduit
2.2.1	Juin 2010	31.12.2011	30.06.2012
2.2.2	Octobre 2010	30.06.2012	31.12.2012
3.0	Avril 2011	30.06.2013	31.12.2013
4.0.3	Novembre 2012	30.06.2014	31.12.2014
4.0.4	Juillet 2013	31.12.2014	30.06.2015

4.8 Exploitation

L'Office fédéral de la statistique (OFS) a mis la plateforme sedex en exploitation en date du 15 janvier 2008. L'OFS a mandaté l'Office fédéral de l'informatique et de la télécommunication (OFIT) pour la partie de l'exploitation sedex. Dans ce cadre là, une SLA (Service Level Agreement) a été conclue entre l'OFS (mandataire) et l'OFIT (prestataire de service) pour l'exploitation de sedex dont les principaux points sont :

Disponibilité du système	96%
Période de service	lundi au vendredi de 7h00 à 18h00 *
Réparation de dérangement	5 heures

Des informations quant aux fenêtres de maintenance prévues, des interruptions constatées et de l'état actuel du système sont disponibles sur le site Internet[11] de l'OFS.

4.9 Frequently Asked Questions (FAQ)

Une foire aux questions[12] a été mise en ligne sur le site Internet de l'OFS et sera mise à jour régulièrement.

En cas de problème, nous vous recommandons de consulter la documentation en ligne avant de contacter le service-clientèle de l'OFS.

[11] http://www.sedex.ch > Exploitation
[12] http://www.sedex.ch > FAQ sedex

5 Compétences

5.1 Service clientèle de l'OFS

5.1.1 Prestations

L'OFS gère un service clientèle à contacter pour les questions suivantes:

- Annonce de nouveaux participants, modification des autorisations ou du routage pour les participants existants
- Questions relatives à l'état de fonctionnement de sedex et au statut des messages
- Demande de modification ou d'extension des fonctions de sedex

Le service clientèle transmet au service compétent (p. ex. sedex Rollout Management) les demandes qu'il n'est pas en mesure de traiter lui-même.

5.1.2 Contact

- Téléphone: 0800 866 700
  E-mail: harm@bfs.admin.ch
- Web: www.registre-stat.admin.ch > Contact
- FAQ: www.sedex.ch > FAQ sedex

5.2 Fournisseur

Le fournisseur d'une application participant à sedex assume les tâches suivantes:

- Développer, tester et entretenir les fonctions des Use Cases traités via sedex conformément aux spécifications définies
- Développer, tester et entretenir l'interface entre l'application et le client sedex, conformément au présent manuel
- Planifier et mettre en œuvre auprès des clients le Rollout de la version nécessaire pour le traitement des Use Cases via sedex, le cas échéant en collaboration avec un exploitant externe
- Former et conseiller (helpdesk) les clients pour le traitement des Use Cases via sedex, le cas échéant en collaboration avec un exploitant externe.

5.3 Participants

Le (futur) participant sedex assume les tâches suivantes:

- Choisir le type de raccordement à sedex (direct ou indirect, voir chapitre 2.4)
- S'annoncer à sedex
- Demander le certificat d'organisation
- Commander la version de l'application requise pour le traitement des nouveaux Use Cases via sedex.

Ces tâches peuvent être déléguées au fournisseur ou à l'exploitant mandaté par ce dernier. Dans tous les cas, il est recommandé de coordonner les activités avec le fournisseur, puisque les participants utilisent en principe sedex par l'intermédiaire d'une application spécialisée.

5.4 Coordination avec un domaine technique

Par «domaine technique», on entend un domaine d'utilisation clairement défini dont certaines fonctions sont assurées par l'intermédiaire de sedex.

5.4.1 Tâches

- Demander à participer au comité de pilotage sedex
- Documenter et publier les Use Cases traités via sedex
- Informer les fournisseurs concernés et les participants potentiels à sedex par l'intermédiaire des Use Cases traités via sedex
- Coordonner les activités nécessaires pour la mise en œuvre des Use Cases via sedex

5.4.2 Coordinateurs actuels des domaines techniques

Domaine technique	Service de coordination
Contrôle des habitants	OFS, Harmonisation des registres
Registre du commerce	OFJ, Domaine de direction Droit privé
e-LP	OFJ, Domaine de direction Services centraux
OFAS	OFAS, Secteur Org. et comptabilité AVS/AI
CSI	Conférence suisse des impôts
ASA 2011	OFAG, Office fédéral de l'agriculture
ASTRA – VU	OFROU, Office fédéral des routes
OVF	OVF, Office vétérinaire fédéral
RP	Institution commune LAMal
ÜDP	ChF, Chancellerie fédérale

6 Test et intégration

6.1 Types de tests

6.1.1 Tests sedex

L'OFS offre la possibilité aux fournisseurs de tester, indépendamment du type de message, si l'application:

- construit les messages de manière syntaxiquement correcte
- construit l'enveloppe correctement
- fournit un fichier de données métier
- est capable de délivrer à l'adaptateur sedex le message correctement (respectivement si l'application est capable de récupérer correctement un message reçu par l'adaptateur sedex)
- permet de tester si les règles d'autorisation et de routage ont été saisies correctement par l'OFS.

L'accent est mis ici sur la communication entre deux adaptateurs sedex. L'interface vers l'application participante ne doit pas être disponible, et le contenu des données métier ne joue aucun rôle.

Le chapitre 6.3 décrit les particularités concernant la constitution du fichier d'enveloppe.

6.1.2 Tests End-to-End

Dans la mesure où le coordinateur du domaine spécialisé l'a prévu, il est possible d'effectuer des tests entre deux systèmes finaux participants. De manière générale, on appliquera la procédure suivante:

- envoi / réception de messages sedex normaux par des instances de test spéciales
- envoi / réception de messages test sedex spéciaux par des instances normales.

Il revient au coordinateur du domaine spécialisé de déterminer la forme dans laquelle les tests E2E sont réalisés.

Dans l'optique d'une auto-certification de l'application, il est recommandé d'utiliser pleinement les possibilités de test offertes (voir chapitre 4.2).

6.2 Instances de tests

Lorsque les tests doivent être réalisés au moyen d'instances de test spéciales, il convient de demander ces dernières auprès du service clientèle de l'OFS.

On fournira en principe les mêmes données que pour l'annonce d'un participant traditionnel (voir chapitre 4.3). Les autorisations et les règles de routage nécessaires aux tests devront, le cas échéant, être précisées.

A noter que sedex n'autorise pas l'échange de messages entre les instances de tests et les instances normales. Cela signifie qu'un Testcase nécessite au moins deux instances de tests.

6.3 Messages de tests

La plateforme sedex donne à ses participants la possibilité de tester l'échange de messages.

Deux méthodes sont à disposition pour effectuer des tests:

- Les messages de test sont échangés à l'aide de participants test (sedex ID = T…)
- Les messages de test sont muni d'un indicateur de test et sont échangés à l'aide de participants productifs

Un échange de messages entre un participant sedex test et un participant sedex productif n'est techniquement pas possible. Cela signifie qu'il n'est pas possible d'envoyer un message à partir d'un participant test vers un participant productif et inversement.

Pour les tests E2E (voir chapitre 6.1.2) réalisés au moyen de participants de test (sender ID / recipient ID = T…), le fichier d'enveloppe ne diffère pas des messages normaux, sauf pour l'identification de l'émetteur et l'identification du destinataire.

Lorsque des participants productifs sont utilisés pour les tests E2E où il n'est pas possible de définir un indicateur de test, le fichier d'enveloppe peut être complété par l'élément XML /eCH-0090:envelope/testData (voir chapitre 3.6).

Cet élément XML permet de joindre un nombre illimité de paramètres de test, accompagnés de toutes les modalités possibles. Les paramètres et leurs modalités doivent être définis par le coordinateur du domaine spécialisé.

6.4 Intégration

L'implémentation des applications dans l'environnement de production ne peut être faite par les fournisseurs que lorsqu'ils ont accompli avec réussite le test et achevé la procédure d'autocertification (voir chapitre 4.2).

7 Sécurité

7.1 Principes de base des réflexions concernant la sécurité

La sécurité des données transmises doit être maximale dans le cadre de sedex. Les principales exigences concernent la confidentialité, l'intégrité et l'assurance de la provenance (authenticité). Ces exigences doivent être assurées de bout en bout (end-to-end) de la transmission entre l'émetteur et le récepteur, même si les données sont envoyées sur des réseaux non protégés.

7.2 Vue d'ensemble du système sedex

Lors de la communication avec la plateforme sedex, les composants suivants fonctionnent ensemble:

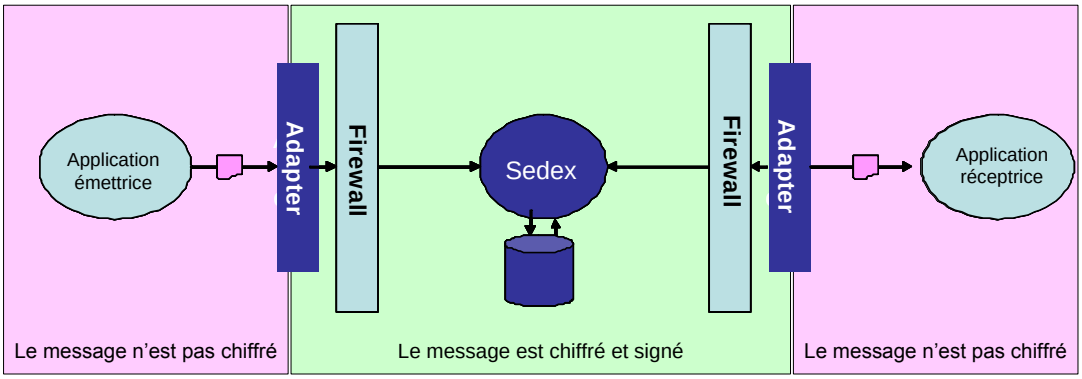


Illustration 20: Composants de la plateforme sedex

La transmission d'un message est réalisée de manière asynchrone :

1. L'application émettrice inscrit les données à transmettre dans un fichier du système local.
2. L'adaptateur de l'émetteur prend le fichier, le signe avec sa clé privée, chiffre les données utiles avec la clé publique du récepteur et transmet le tout à sedex. Le système sedex stocke les données transmises tel qu'il les a reçues, c'est-à-dire chiffrées.
3. L'adaptateur du récepteur vérifie à intervalles réguliers si des messages à son attention sont déposés auprès de sedex. Si c'est le cas, il récupère ces messages.
4. L'adaptateur du récepteur déchiffre les données avec la clé privée du récepteur, vérifie la signature de l'émetteur et dépose le message reçu comme fichier dans le système local.
5. Avant tout traitement, le message reçu peut encore faire l'objet de vérifications supplémentaires par le récepteur (par ex. recherche de virus, etc.).
6. L'application réceptrice lit le fichier et en vérifie la conformité avec le schéma XML correspondant.

La collaboration avec sedex exige des émetteurs et récepteurs que soient remplies les conditions suivantes :

- installation du client
- installation du certificat d'organisation (X509.v3)
- un canal de communication électronique (TCP/IP; HTTP, HTTPS) doit être disponible pour communiquer avec sedex

- dans le firewall, les ports 80 (HTTP) et 443 (HTTPS) doivent être ouverts pour des liaisons sortantes. Etant donné que sedex n'établit jamais de liaison avec un adaptateur en réception, aucun port ne doit être ouvert pour un flux de données entrant.

Indépendamment de sedex, les environnements locaux doivent naturellement aussi prendre les mesures de sécurité adéquates (voir chapitre 7.3). Les types de raccordement logiques sont spécialement exposés à un risque de sécurité. L'OFS recommande donc de préférer dans la mesure du possible les raccordements physiques aux raccordements logiques.

Remarque: le système sedex utilise pour l'échange de données le produit Governikus de la maison Bremen Online Services. Ce produit a été vérifié sur le plan de sa sécurité par l'Office fédéral pour la sécurité dans les technologies d'information du gouvernement allemand.

7.3 Attente à l'égard des applications participantes

Dans la sécurité de l'exploitation, les fournisseurs de logiciel doivent répondre aux exigences suivantes :

- Le logiciel doit utiliser le client sedex selon les conditions décrites dans ce manuel. Il n'est pas permis d'implémenter des solutions d'évitement qui pourraient mettre en danger la sécurité.
- L'ordinateur sur lequel est installé le logiciel doit bénéficier d'un niveau de protection élevé. En font partie:
  - une protection contre les virus mise à jour automatiquement
  - l'actualisation immédiate de l'installation si des lacunes de sécurité sont détectées
  - un accès réservé exclusivement aux personnes qui en ont besoin pour exercer leur fonction
  - la déconnexion des services qui ne sont pas utilisés par le système d'exploitation
  - la limitation des accès au réseau aux seuls protocoles utilisés dans l'exploitation. Cela concerne en particulier l'accès à des réseaux qui ne sont pas sous la responsabilité directe de l'organisation concernée.

7.4 Evaluation des risques de sécurité pour l'émetteur et le récepteur

L'évaluation des risques de sécurité pour l'émetteur et le récepteur a été réalisée par l'Unité de pilotage informatique de la Confédération (UPIC). Le résultat est à disposition (document en allemand) à l'adresse http://www.sedex.ch.

7.5 Composants de la sécurité - certificats de sécurité

La sécurité des données au cours de leur transfert est assurée dans sedex au moyen de la technologie Public key, avec utilisation de certificats d'organisation délivrés par AdminPKI (voir aussi le site http://www.pki.admin.ch). La protection des données traitées exige cependant aussi que l'ordinateur sur lequel sont préparées les données avant leur transfert soit également sécurisé. Cette protection est importante dans la mesure où les données sont ici sans protection aucune et que les éléments secrets (private key) sont également installés sur cet ordinateur.

Important: la sécurité de ces composants pourrait être compromise si une personne non autorisée pouvait y accéder.

7.6 Renouvellement des certificats de sécurité

7.6.1 La problématique de la mise à jour des certificats de sécurité

La plate-forme sedex nécessite plusieurs types de certificats pour son fonctionnement. Les certificats de sécurité (serveur et client) sedex sont valables 3 ans. Ce document traite seulement deux types de certificats qui sont directement touchés par cette date d'expiration et l'utilisation de la fonctionnalité du renouvellement automatique :

1. le certificat d'organisation de l'adaptateur sedex
2. le certificat de transport et les truststores du serveur sedex.

Pour permettre la mise à jour de ces certificats, le client sedex doit fonctionner sans interruption pendant au moins 24 heures.

Il n'est pas possible de transmettre un message sur la plateforme sedex sans certificat valable.

7.6.1.1 Certificat d'organisation de l'adaptateur sedex

Le certificat d'organisation est celui qui est installé sur la machine du client et qui est utilisé par le client sedex. Il sert à signer et crypter les données envoyées et reçues par le participant physique de sedex. Ce type de certificat est délivré par l'OFS lors de la création et de la configuration initiale d'un nouveau participant physique.

Certificats de test

La fonctionnalité de renouvellement automatique des certificats n'a pas été implémentée pour les participants tests (sedex Id commençant par un TX-XXX-X). Ce type de certificat, qui a également une durée de 3 ans, doit être renouvelé manuellement en collaboration avec l'OFS.

Pour ce faire, la personne responsable du certificat doit faire une demande de prolongation à l'OFS (Service clientèle de l'harmonisation des registres : harm@bfs.admin.ch) 60 jours avant l'expiration des certificats. La date d'expiration peut être trouvée très facilement par la personne responsable du certificat (voir chapitre 8.4.4).

Si aucune demande de prolongation du certificat de test n'a été faite au service clientèle, l'OFS ne renouvellera pas le certificat. Après la date d'expiration, il ne sera plus possible de transmettre des messages avec ce certificat.

7.6.1.2 Certificat de transport et truststores du serveur sedex

Le certificat de transport et les truststores du serveur sedex sont livrés avec le client sedex. Ces certificats servent à identifier de manière certaine le serveur sedex, de façon à empêcher la connexion à des serveurs quelconques. Ce type de certificat est généré par l'OFIT et renouvelé automatiquement et au même moment par tous les participants sedex (y compris les participants tests).

8 Annexe

8.1 Schémas XML

Par le passé, L'OFS mettait à disposition sur son site Internet les schémas XML pour l'enveloppe sedex, la quittance sedex, ainsi que pour les différents use cases utiles dans le cadre de l'harmonisation des registres.

Etant donné que les schémas XML sont entre-temps publiés sur le site Internet de l'association eCH, l'OFS renonce à publier à l'avenir son propre jeu de schémas XML.

Les schémas sont désormais téléchargeables à l'adresse suivante: http://www.ech.ch/xmlns

8.2 Règles pour les documents XML

8.2.1 Codage des documents XML

Le codage de tous les documents XML échangés devrait être UTF-8 conformément aux recommandations d'eCH et de la norme eCH-0018 (XML Best Practices). Si UTF-8 n'est pas utilisé, il faut indiquer l'encodage correpondant dans la déclaration de XML («encoding»). À cause du volume de données supplémentaires (chaque signe nécessite 2 octets !) il faut renoncer à l'utilisation d'UTF-16 pour le codage.

8.2.2 Indications de temps

Toutes les indications de temps dans les documents XML (types de données XML : xs:datetime et xs:time) doivent contenir des indications sur le fuseau horaire, soit sous forme hh:mm:ssZ, soit hh:mm:ss(+|-)hh:mm. Si l'indication du fuseau horaire manque, les indications de temps ne sont pas déterminées complètement.

Nous recommandons de formuler toutes les indications d'heure ou de date au format UTC.

8.3 Service web CheckSedex

Lorsqu'un participant souhaite envoyer un message à un autre service administratif, il ne sait pas s'il peut envoyer ce message via sedex ou s'il doit rechercher un autre moyen de transmission pour ce message, par exemple la voie postale. C'est la raison pour laquelle il est possible de consulter le service web CheckSedex avant la transmission d'un message.

8.3.1 Description du service

Le service CheckSedex confronte les éléments principaux de l'enveloppe du message (émetteur, type de message, classe de message, récepteur) à la liste des participants et effectue une procédure d'autorisation.

Pour les raisons suivantes, il est possible que le participant ne puisse pas envoyer de message via sedex :

- le service administratif de l'émetteur ou du destinataire n'est pas activé en tant que participant à sedex
- l'émetteur mentionné dans l'enveloppe n'est pas habilité à envoyer le type de message (autorisation de l'émetteur)

- le destinataire n'est pas en mesure de traiter le type de messages envoyés (autorisation du destinataire)
- l'adaptateur émetteur (émetteur physique) n'est pas autorisé à envoyer le message (autorisation de l'émetteur)
- l'un des destinataires n'a pas le certificat valable nécessaire pour crypter le message
- erreur dans l'enveloppe: l'émetteur, l'ID de l'adaptateur, le type de message ou le destinataire comporte une erreur
- La taille du fichier métier dépasse la limite maximale autorisée (champ optionnel)

L'ID de l'adaptateur est nécessaire car certaines règles d'autorisation utilisent également l'identité de l'adaptateur qui envoie le message ; il s'agit de l'identité de l'émetteur physique.

8.3.2 Limitations

Ce service web peut être utilisé pour tous les envois à effectuer via sedex, mais il est surtout utile dans le cadre d'échanges intercommunaux, et plus généralement lorsque le cercle de participants évolue (p. ex pour les messages de déménagement entre registres des habitants).

Lors de la réponse, le service web se base uniquement sur les types de messages autorisés pour un participant. Les versions de schémas XML supportées par les participants n'entrent donc pas en considération.

Il est également possible d'interroger les services web de l'annuaire des participants Event Bus Suisse (EBS-Dir) qui fourni les types de messages et les versions de schémas XML supportés par les participants.

8.3.3 Configuration requise

Le service web CheckSedex exige l'utilisation d'un certificat pour chiffrer la communication. Pour utiliser ce service, il est donc nécessaire d'utiliser le proxy service web.

Il est également possible d'implémenter les mécanismes de sécurité directement dans l'application participante, il n'est dès lors plus nécessaire d'utiliser le proxy service web.

8.3.4 Paramètres d'envoi

Nom d'attribut	Type	Mandatory	Description
Sender	sedex ID	Oui	ID de l'émetteur (émetteur dans l'enveloppe)
AdapterID	sedex ID	Oui	ID de l'adaptateur qui doit envoyer les données
MessageType	Numérique	Oui	Type de message
MessageClass	Numérique	Oui	Classe de message
MessageSize	Numérique	Non	Taille du fichier métier en octets
Recipients	Liste des sedex ID	Oui	Liste des destinataires (dans l'enveloppe)

8.3.5 Paramètres de réponse

Nom d'attribut	Type	Description
Result	Numérique	0: YES (= message valable et autorisé) 1: NO (= le message ne peut pas être envoyé, voir code d'erreur)
ErrorCode	Numérique	100: (OK - no error) 300: Unknown sender id %s 301: Unknown recipient id %s ** 302: Unknown physical sender id %s 303: Invalid message type %s 304: Invalid message class %s 310: Not allowed to send 311: Not allowed to receive ** 312: User certificate not valid ** 330: Message size exceeds limit ** 999: Other (détails sous Attribut ErrorMessage) ** voir RecipientAuthResult pour un résultat par récepteur
ErrorMessage	String	Message d'erreur, si ErrorCode > 0.
RecipientAuthResult	RecipientAuthResult[]	Liste comprenant les autorisations pour chaque destinataire. Existe seulement si ErrorCode contient un des codes suivants: 301, 311, 312, 330

Typ RecipientAuthResult:

Nom d'attribut	Type	Description
RecipientSedexId	string	ID sedex pour lequel le résultat s'applique
RecipientResult	Numérique	0: YES (= le récepteur est autorisé) 1: NO (= le message ne peut pas être envoyé à ce récepteur, voir motif sous RecipientErrorCode)
RecipientErrorCode	Numérique	100: (OK - no error) 301: Unknown recipient id %s 311: Not allowed to receive 312: User certificate not valid 330: Message size exceeds limit
RecipientErrorMessage	String	Message d'erreur si RecipientErrorCode > 0

Voir le chapitre 3.9.2 pour la signification des codes d'erreur.

8.4 Processus standard pour la distribution de certificats d'organisation

8.4.1 Première distribution et renouvellement manuel

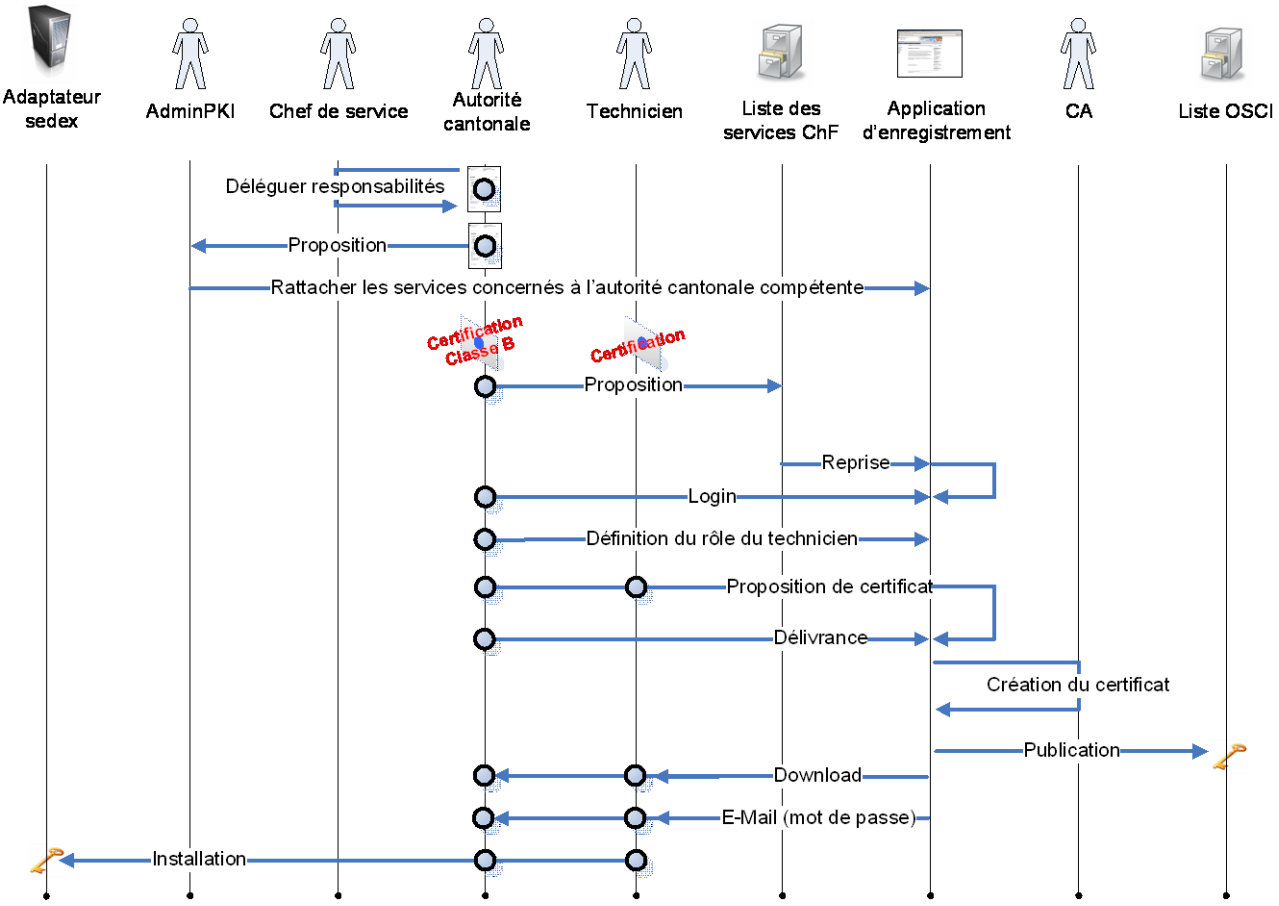


Illustration 21: Processus standard de distribution centralisée des certificats d'organisation

8.4.2 Renouvellement automatique

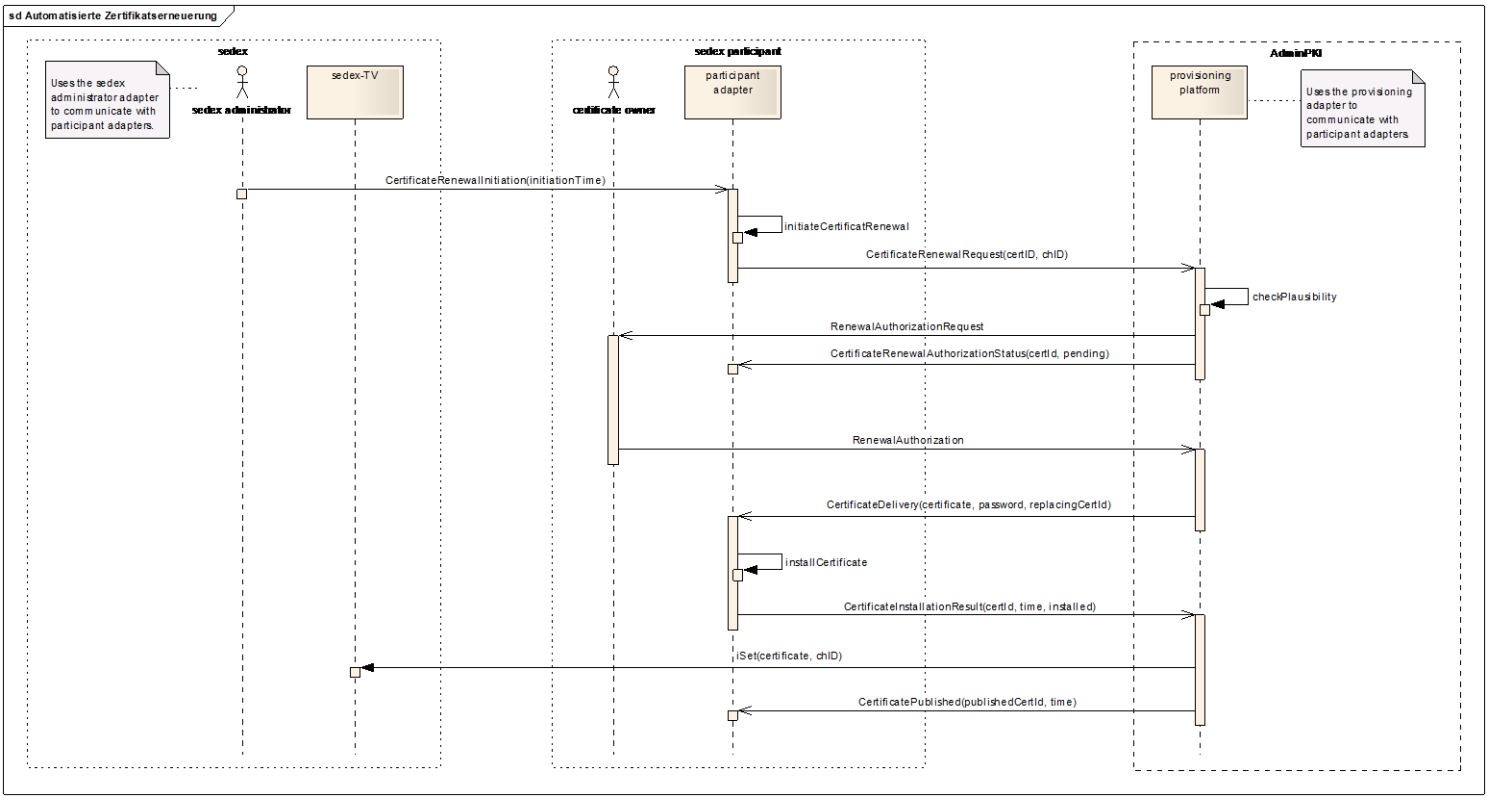


Illustration 22: Processus standard du renouvellement automatique du certificat

8.4.3 Inconvénients du renouvellement manuel du certificat

Le processus n'est pas déclenché par le système, mais initié par le participant sedex.

Le transport du certificat d'organisation depuis l'application génératrice d'Admin PKI jusqu'au participant sedex est une procédure longue, lourde et coûteuse.

La clef publique est publiée immédiatement après la commande, et non pas suite à l'installation du certificat. Les messages adressés durant ce laps de temps au participant ne pourront pas être téléchargés.

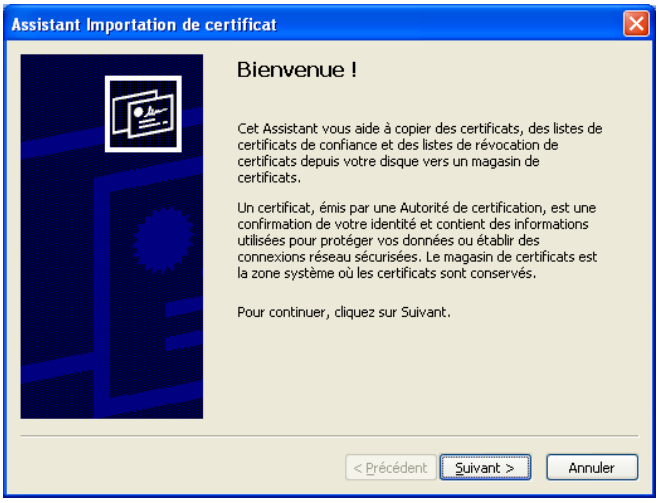
Le renouvellement manuel du certificat nécessite un redémarrage de l'adaptateur.

8.4.4 Procédure pour retrouver la date d'expiration du certificat d'organisation

1

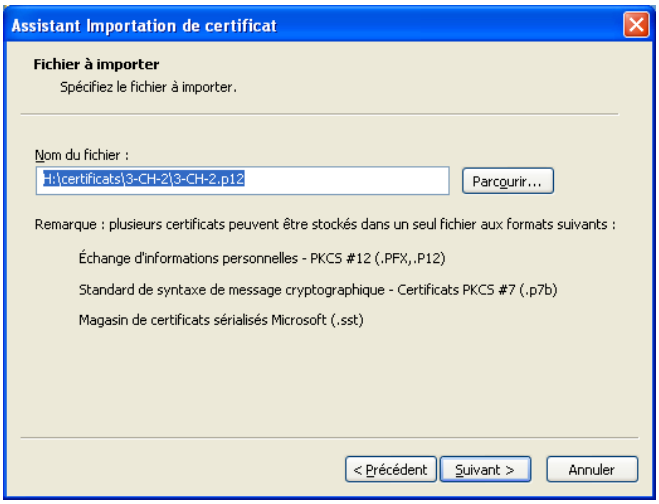
Dans ***l'Explorateur Windows***, double-cliquer sur le certificat pour lequel la date d'expiration doit être découverte.

2


Assistant Importation de certificat
Bienvenue !
Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation de certificats depuis votre disque vers un magasin de certificats.
Un certificat, émis par une Autorité de certification, est une confirmation de votre identité et contient des informations utilisées pour protéger vos données ou établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.
Pour continuer, cliquez sur Suivant.
< Précédent
Suivant >
Annuler

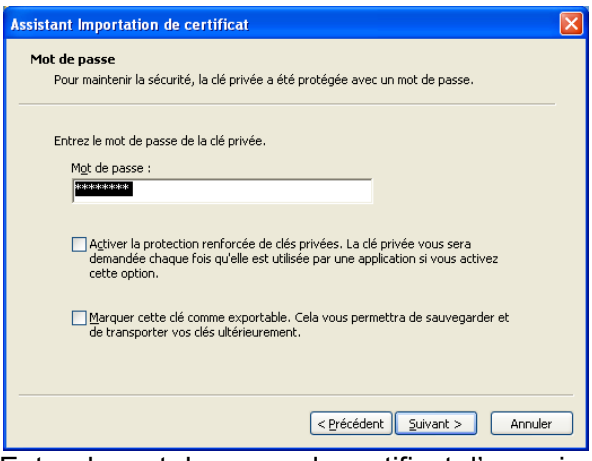
Ecran d'introduction.
Cliquer sur ***Suivant***.

3


Assistant Importation de certificat
Fichier à importer
Spécifiez le fichier à importer.
Nom du fichier :
H:\certificats\3-CH-2\3-CH-2.p12
Parcourir...
Remarque : plusieurs certificats peuvent être stockés dans un seul fichier aux formats suivants :
Échange d'informations personnelles - PKCS #12 (.PFX,.P12)
Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.p7b)
Magasin de certificats sérialisés Microsoft (.sst)
< Précédent
Suivant >
Annuler

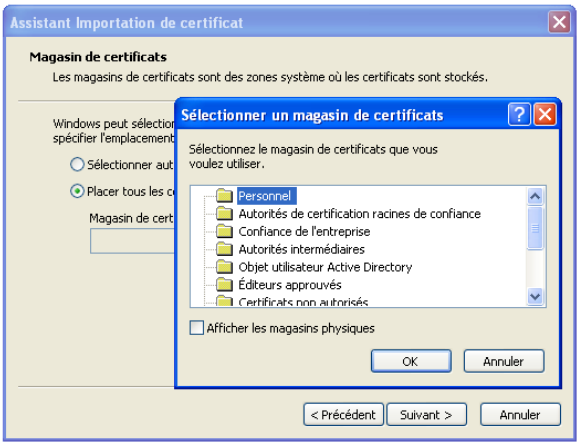
Le certificat choisi est affiché par défaut.
Cliquer sur ***Suivant***.

4


Assistant Importation de certificat
Mot de passe
Pour maintenir la sécurité, la clé privée a été protégée avec un mot de passe.
Entrez le mot de passe de la clé privée.
Mot de passe :
Activer la protection renforcée de clés privées. La clé privée vous sera demandée chaque fois qu'elle est utilisée par une application si vous activez cette option.
Marquer cette clé comme exportable. Cela vous permettra de sauvegarder et de transporter vos clés ultérieurement.
< Précédent
Suivant >
Annuler

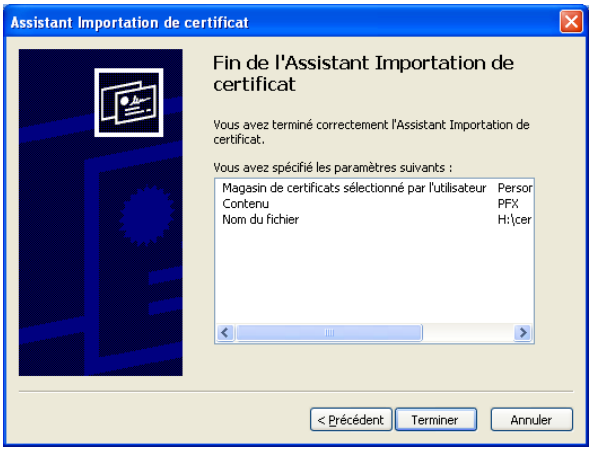
Entrer le mot de passe du certificat d'organisation
(défini dans le fichier conf/password.txt ou conf/certificateConfiguration.xml).
Cliquer sur ***Suivant***.

5



Cliquer sur ***Parcourir*** et sélectionner le magasin de certificats « ***Personnel*** ».
Cliquer sur ***Suivant***.

6


Assistant Importation de certificat
Fin de l'Assistant Importation de certificat
Vous avez terminé correctement l'Assistant Importation de certificat.
Vous avez spécifié les paramètres suivants :
Magasin de certificats sélectionné par l'utilisateur Persor
Contenu PFX
Nom du fichier H:\cer
< Précédent
Terminer
Annuler

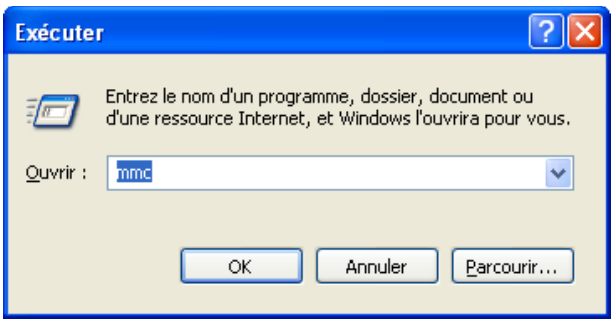
Cliquer sur ***Terminer***.

7

Cliquer sur ***OK***.

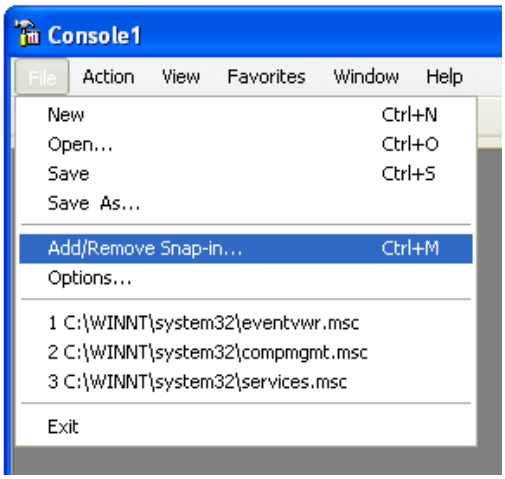
8 ➔ ***Exécuter***

9



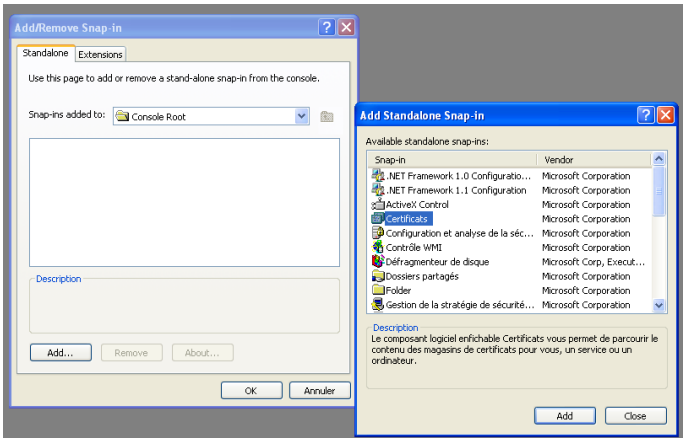
Taper "MMC".
Cliquer sur ***OK***.

10



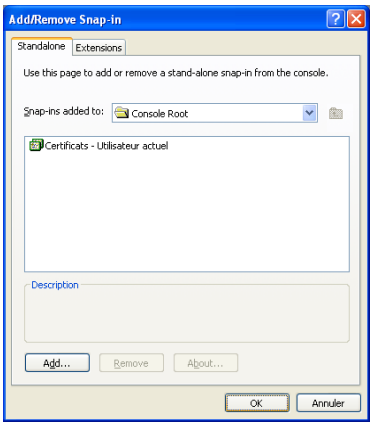
Cliquer sur ***File*** et sélectionner ***Add/Remove Snap-in***.

11



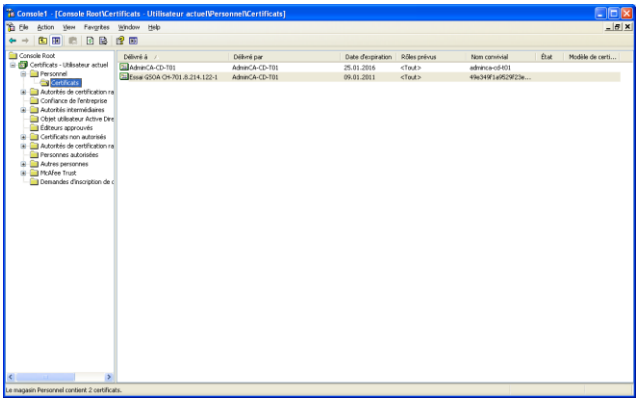
Cliquer sur ***Add*** et sélectionner le Snap-in « ***Certificats*** ».
Cliquer ensuite sur ***Add*** puis ***Close***.

12



Confirmer le choix du Snap-in en cliquant sur ***OK***.

13



Le certificat et sa date d'expiration apparaissent sous
↳ Certificats – Utilisateur actuel
↳ Personnel
↳ Certificats

8.5 Fichier logs

Ce chapitre décrit les fichiers logs pour le client sedex (controller, adaptateur et proxy service web).

8.5.1 Contexte

Dans le cadre de son exploitation, le client sedex génère des logs. Ceux-ci permettent à tous les exploitants de mieux comprendre le comportement de l'adaptateur sedex, tout en permettant aux administrateurs sedex de continuer à accéder aux informations techniques les concernant.

Les fichiers de log ont été créés de façon à séparer les informations techniques des informations pouvant servir au participant pour suivre les messages sedex. Cette séparation permet au participant de mieux comprendre le comportement de l'adaptateur sedex, sans pour autant sacrifier de précieux détails dans le log technique, destiné aux administrateurs sedex dans le cadre du support.

8.5.2 Description des fichiers

Voici à quoi correspond chacun des fichiers de log:

- **Log technique**
  Correspond au fichier log actuel.
- **Log d'erreur**
  Contient toutes les erreurs détectées par l'adaptateur. Les erreurs se rapportant à un message sont identifiées par un code permettant de suivre le message.
- **Log de réception**
  Contient la liste des messages reçus. Chaque enregistrement de ce log est identifié par différentes informations, telles que l'identifiant du message correspondant.
- **Log d'envoi**
  Contient la liste des messages envoyés et des quittances reçues. Chaque enregistrement de ce log est identifié par différentes informations, telles que l'identifiant du message correspondant.

8.5.3 Logs du controller

8.5.3.1 Le log technique (controller-technical.log)

Généralités
Ce log comprend différentes informations concernant l'état et la surveillance des composants (adaptateur et proxy service web), des informations administratives (version du controller, sedex ID, etc.[14]) et quelques détails spécifiques au controller (notamment les paramètres des cronexpressions[15]).

Langues
Exclusivement en anglais.

Formatage
```
AAAA-MM-JJ HH:MM:SS LEVEL [THREAD] Txt
```

Exemples
- Sedex ID utilisé:
```
2012-03-19 08:41:06,027 INFO [main] ch.admin.bit.sedex.controller.main.ControllerEngine:
➥ Using sedexID 3-CH-10
```
- Signalement de la version du controller au serveur sedex:
```
2012-03-19 08:41:44,130 INFO [main] ch.admin.bit.sedex.controller.configuration.ConfigurationClient:
➥ Submitting Controller - Version was successful
```

8.5.4 Logs de l'adaptateur

8.5.4.1 Log technique (adapter-technical.log)

Généralités

Contrairement aux trois autres logs (d'erreur, de réception, d'envoi), celui-ci ne comprend pas d'informations permettant d'identifier un message sedex.

Langues

Anglais principalement, parfois allemand.

Formatage
```
AAAA-MM-JJ HH:MM:SS LEVEL [THREAD] Txt
```

Exemples

- Chargement du profil (premier enregistrement lors du démarrage):
```
2012-05-11 15:57:39,369 INFO [main]
➥ ch.admin.bit.sedex.utils.AdapterConfigurationReader: Loading Performance Profile small
```
- Pas de nouveaux messages à envoyer (outbox vide):
```
2012-04-23 12:07:46,837 DEBUG [GlobalAdapterScheduler_Worker-0]
➥ ch.admin.bit.sedex.scheduler.ThrottlingPriorityMessageScheduler: No new messages in outbox.
```

[14] Aussi date d'échéance du certificat, chemin d'installation du client sedex, monitoring, état des interrupteurs, indications sur le proxy service web, module *keepalive*, module *agent*.
[15] Une cronexpression (expression cron) est un paramètre généré par le programme *cron*. Celui-ci permet notamment d'exécuter des commandes à un moment déterminé. Les paramètres spécifiés ne sont pas modifiables par l'utilisateur du client sedex.

8.5.4.2 Log d'erreur (adapter-error.log)

Généralités

Ce log liste les erreurs de manière lisible et compréhensible.

Si l'erreur se rapporte à un message sedex reçu ou envoyé, les différentes informations permettant d'identifier ce message sont indiquées.

Les erreurs métier de l'adaptateur (autorisation refusée, date du message trop ancienne, etc.) autant que les erreurs techniques (pas de connexion, dossier inexistant, etc.) sont clairement indiquées et sont accompagnées d'un numéro d'erreur permettant un meilleur support en cas de problème.

Exception: Pour les erreurs liées à des problèmes de connexion, les détails du message ne peuvent pas être affichés.

Liste des erreurs

Selon le chapitre «Généralités», les erreurs listées dans ce log sont détaillées et comportent un numéro d'erreur.

Les différentes erreurs possibles sont répertoriées dans le chapitre 8.5.7.1.

Langues

Exclusivement en anglais.

Formatage

- Lorsqu'il s'agit d'un message sedex:
  `AAAA-MM-JJ HH:MM:SS MsgId SenderId RecipientId UsmId CommonMsgId Txt`
- Si une information est manquante (p.ex. UsmId), le tiret "–" est utilisé:
  `AAAA-MM-JJ HH:MM:SS MsgId SenderId RecipientId - CommonMsgId Txt`
- Lorsqu'il s'agit d'un événement général qui ne se rapporte pas à un message précis:
  `AAAA-MM-JJ HH:MM:SS Txt`

Exemples

- Lorsqu'il s'agit d'une erreur connue et numérotée:
  ```
  2012-04-24 15:58:56 20120424155711 T3-CH-31 T3-CH-42 209954536 testsedex02
  ➥ Error #A30001: The participant does not have sufficient
  ➥ credentials to receive a message with this message type.
  ```
- Lorsque l'erreur n'est pas répertoriée:
  ```
  2011-05-18 16:48:07 2011xxyyzz 3-CH-2 3-CH-9 201949899 2011xxyyzz
  ➥ Error #A999: An unexpected generic error occurred. Check technical log for further details.
  ```

8.5.4.3 Le log de réception (adapter-receive.log)

Généralités

Les messages que l'adaptateur a reçus ainsi que leur statut sont loggés ici. Les informations inscrites permettent d'identifier le message.

Les éventuelles erreurs lors de la réception d'un message sont mentionnées de manière générique (pas de précision dans ce log) ; les détails figurent dans le log d'erreur (voir chapitre 8.5.4.2).

Les différents destinataires pertinents pour l'adaptateur sont indiqués sous forme de liste séparée par le caractère point-virgule ";". Cette liste est indiquée dans le champ `RecipientId`.

Cardinalité

Ce log comporte dans tous les cas un seul enregistrement, indépendamment du nombre de destinataires.

Les différents destinataires pertinents pour l'adaptateur sont indiqués sous forme de liste séparée par le caractère point-virgule ";". Cette liste apparaît dans le champ `RecipientId`.

Langues

Exclusivement en anglais.

Formatage

- Il est construit de la façon suivante:
  `AAAA-MM-JJ HH:MM:SS MsgId SenderId RecipientId UsmId CommonMsgId Txt`
- Lorsqu'une information est manquante (p.ex. *UsmId*), le tiret "–" peut être utilisé:
  `AAAA-MM-JJ HH:MM:SS MsgId SenderId RecipientId - CommonMsgId Txt`

Exemples

- `2011-05-18 16:19:54 2011xxyyzz 3-CH-2 3-CH-11 201949185 2011xxyyzz`
  `➥ Message successfully received.`
- `2011-05-18 16:19:54 2011xxyyzz 3-CH-2 3-CH-11;3-CH-12 201949185 2011xxyyzz`
  `➥ Message successfully received.`
- `2011-05-18 17:53:27 2011xxyyxz 3-CH-2 3-CH-11 201949902 2011xxyyxz`
  `➥ Message could not be received. Check error log and technical log for further details.`

8.5.4.4 Le log d'envoi (adapter-send.log)

Généralités

Ce log liste les différents messages envoyés, le statut de chaque message ainsi que les quittances reçues par l'adaptateur.

Les informations inscrites permettent d'identifier le message.

Les éventuelles erreurs lors de l'envoi d'un message sont mentionnées de manière générique ; les détails sont indiqués dans le log d'erreur (voir chapitre 8.5.4.2).

Lorsque l'enveloppe sedex du message à envoyer n'est pas lisible, l'adaptateur tente malgré tout de lire le message ID et l'expéditeur de l'enveloppe, afin de pouvoir générer une quittance minimale.

Langues

Exclusivement en anglais.

Formatage

- Il est construit de la façon suivante:
  `AAAA-MM-JJ HH:MM:SS MsgId SenderId RecipientId UsmId CommonMsgId Txt`
- Lorsqu'une information est manquante (p.ex. *UsmId*), le tiret "–" peut être utilisé:
  `AAAA-MM-JJ HH:MM:SS MsgId SenderId RecipientId - CommonMsgId Txt`

Exemples

- `2011-05-18 15:21:09 2011xxyyxx 3-CH-2 3-CH-11 201949831 2011xxyyxx`
  `➥ Message successfully sent to the server.`
- `2011-05-18 15:32:41 2011xxyyxx 3-CH-2 3-CH-11 201949831 2011xxyyxx`
  `➥ Message received by the recipient (100 Message successfully transmitted).`

- 2011-05-18 16:47:13 - 3-CH-2 - - 2011xxyyxv
  ➥ Message cannot be read. Check error log and technical log for further details.
- 2011-05-18 17:53:27 2011xxyyxz 3-CH-2 3-CH-11 201949902 2011xxyyxz
  ➥ Message could not be sent (310 Not allowed to send).
  ➥ Check error log and technical log for further details.

8.5.5 Logs du proxy service web

8.5.5.1 Le log technique (wsproxy-technical.log)

Généralités

Il ressemble au log que nous avions dans les versions précédentes du proxy service web, lorsque celui-ci était démarré sans le wrapper.

Ce log contient la retranscription de tous les paramètres de configuration spécifiques à ce composant sedex (notamment la version, les cronexpressions, l'état actuel, etc.) mais également de précieuses informations en cas d'erreur.

Langues
Anglais principalement, parfois allemand.

Formatage

```
AAAA-MM-JJ HH:MM:SS LEVEL [THREAD] Txt
```

Exemples

- Démarrage (premier enregistrement):
  ```
  2012-04-23 12:01:29,842 INFO [main]
  ➥ ch.admin.bit.sedex.wsproxy.server.WsProxyServer -
  ➥ [WsProxyServer] Starting WsProxy Version WSP 4.0.1
  ```
- Temps total de fonctionnement (processus d'arrêt):
  ```
  2012-04-24 16:07:30,012 INFO [Common ws proxy scheduler_Worker-5]
  ➥ ch.admin.bit.sedex.wsproxy.server.WsProxyServer -
  ➥ WSProxy uptime was 00:07:15
  ```

8.5.5.2 Le log d'accès (wsproxy-access.log)

Généralités

Ce log mentionne tous les accès (requêtes) effectués par le proxy service web.

En cas d'erreur (p.ex. accès refusé), celle-ci est reportée de manière claire dans ce log, en mentionnant les numéros d'erreur correspondants.

A noter que les détails d'une erreur se trouvent dans le log technique.

Langues
Exclusivement en anglais.

Formatage

```
AAAA-MM-JJ HH:MM:SS DURATION CLIENT RESULT_CODE REQ_BYTES RSP_BYTES REQ_ENDPOINT REQ_METHOD ORIG_REQ[16]
➥ [OPT FIELDS]
```

Exemples

- Requête CheckSedex:
  ```
  2012-05-24 11:22:09.614 31 10.147.132.133 OK 555 182
  ```

[16] Pour davantage de détails sur les champs, consulter le tableau du point 8.5.7.2.

```
➥ https://www.sedex-gw.admin.ch/sedex-runtime-ws/CheckSedexWebService
➥ checkSedex 10.147.132.133/wsproxy/services/CheckSedexWebService/
```

- Requête non autorisée via le service web UPIQuery:

```
2012-04-11 12:07:47.966 422 10.147.13x.xxx
➥ Fault_when_calling_target_service 355 400
➥ https://wupi.zas.admin.ch/wupi_cc/UPIQueryService getInfoPerson
➥ 10.147.13x.xxx/wsproxy/services/UPIQueryService/
```

- Requête autorisée via le service web UPIQuery:

```
2012-05-24 10:44:05.390 2265 10.147.13x.xxx OK 316 2007
➥ https://wupi.zas.admin.ch/wupi_cc/UPIQueryService getInfoPerson
➥ 10.147.13x.xxx/wsproxy/services/UPIQueryService/
```

8.5.6 Configuration

Il est possible de configurer le nombre de fichiers logs (d'archives) à écrire ainsi que leur taille. Si les limites sont atteintes, les logs existants sont "roulés"[17]. Chacun des fichiers log est configurable indépendamment des autres.

8.5.6.1 Emplacements et valeurs par défaut

Le client sedex accueillera probablement d'autres modules dans le futur. Cette logique modulaire s'applique également aux fichiers log, dont voici les paramètres par défaut:

	Emplacement	Roulement	Fichier de configuration
Adaptateur	ClientDir/logs/adapter/	5 fichiers de 10 Mo	adapter-log4j.xml (ClientDir/adapter/conf/)
Proxy service web	ClientDir/logs/wsproxy/	5 fichiers de 10 Mo	wsproxy-log4j.xml (ClientDir/adapter/conf/)
Controller	ClientDir/logs/controller/	5 fichiers de 10 Mo	controller-log4j.xml (ClientDir/controller/conf/)

8.5.7 Annexes

8.5.7.1 Liste des erreurs du log d'erreur

Catégories d'erreur

Le log d'erreur affiche des informations détaillées et compréhensibles. Pour permettre aux exploitants de réagir de manière adéquate à un défaut, des catégories d'erreur ont été introduites. Les catégories présentées ci-dessous forment un sur-ensemble des catégories utilisées pour les quittances sedex (voir chapitre 3.9.1).

Plage de numéro	Catégorie
20'000 – 29'999	Erreur de message/appel service web permanente
30'000 – 39'999	Erreur d'autorisation permanente
40'000 – 49'999	Erreur de transport temporaire
50'000 – 59'999	Erreur de l'adaptateur/webservice-proxy temporaire
80'000 – 89'999	Erreur de l'adaptateur/webservice-proxy permanente
90'000 – 99'000	Erreur de configuration de l'adaptateur/webservice-proxy

Exemple: A80006

[17] «Rolled» en anglais. Réécriture circulaire des fichiers présents (par défaut, 1 fichier « principal » et 5 fichiers d'archive).

Liste des erreurs de l'adaptateur

La liste suivante présente les erreurs prévues pour le log d'erreur de l'adaptateur sedex :

Numéro	Erreur
A20000	No payload was found. Please join a payload to this envelope and retry again.
A20001	The given envelope is not valid. Please make sure that this envelope corresponds to the XML schema eCH-0090 (Reason: [reason]).
A20002	The message cannot be sent as the envelope and the content file cannot be found in folder [folder].
A30000	The participant does not have sufficient credentials to send a message with this message type.
A30001	The participant does not have sufficient credentials to receive a message with this message type.
A30002	The participant does not exist (this happens when the participant has not been activated or if he is unknown in the sedex system).
A30003	The authorization check failed for following reason: [StatusInfo from eCH-0090:Receipt]
A30004	The organization certificate renewal process cannot take place as the participant has a test ID.
A40000	Some of the addresses (URL: [URL]) that are needed in order to communicate with the server are not available.
A40001	There is an unreadable HTTPS answer. This is usually caused by an unexpected response from the server (e.g. a HTML response generated by a web proxy or if a network component changed the request).
A40002	The server received an invalid OSCI request. This is usually caused by a corrupted request from the client (e.g. when using an old transport certificate or if a network component changed the request).
A40003	There is an unreadable OSCI answer. This is usually caused by an unexpected response from the server (e.g. a HTML response generated by a web proxy or if a network component changed the request).
A80000	The organization certificate is expired. Please install a valid organization certificate and retry again.
A80001	The organization certificate renewal cannot take place: [Problem]
A80002	The transport certificate renewal cannot take place: [Problem]
A80003	The truststore update cannot take place: [Problem]
A80004	An old transport certificate is used. Please install a validate transport certificate and retry again.
A80005	The sedex-adapter cannot start as another instance is probably already running. Please stop the sedex-adapter and retry again after 5 minutes.
A80006	The sedex-adapter cannot start as another instance is using the database. Please stop the sedex-adapter and retry again after 5 minutes.
A80007	There are not enough privileges to write on the folder [Folder]. Please check the privileges and restart the sedex-adapter.
A90000	The sedex-adapter ID does not match with the organization certificate.
A90001	The password does not match with the organization certificate.
A90002	The organization certificate cannot be found within the given path.
A90003	The JCE extension is not installed in the Java Runtime Environment (JRE).
A90004	Some of the data folders ([dataFolder]: [pathToDataFolder]) are not available or there is not enough space left.
A90005	The temp folder [tempFolderPath] is not available or there is not enough space left.
A90006	Could not move test file from outbox to sedextempmessage folder. Use parameter processingDir in file sedexadapter.properties to define a new location for the sedextempmessage folder which is on the same disk as the outbox folder.

Numéro	Erreur
A90007	Could not move test file from sedextempmessage to sent folder. Use parameter sentItemsDir in file sedexadapter.properties to define a new location for the sent folder which is on the same disk as the sedextempmessage folder.
A90008	The certificate configuration file is not readable (given reason: [Reason]). Please make sure that this configuration file corresponds to the XML schema.

8.5.7.2 Liste des champs du log d'accès du proxy service web

Champ	Description
`date`	Date de l'enregistrement au format ISO 8601: YYYY-MM-DD Ex: `2004-07-11`
`time`	Heure de l'enregistrement au format ISO 8601: hh:mm:ss.f Ex: `16:43:16.234`
`duration`	Durée de l'appel (Round Trip Time) en millisecondes. Ex: `129`
`client`	Adresse IP du client qui appelle. Ex: `192.128.30.22`
`result-code`	Code de résultat (chaine de caractères). Exemples: `OK` Réponse standard pour appels réussis. `Fault_HTTP_Get_Not_Allowed` Faute SOAP avec indication sur le type de faute.
`req-bytes`	Nombre de bytes de la requête SOAP.
`rsp-bytes`	Nombre de bytes de la réponse SOAP.
`req-endpoint`	Point de destination (URL) du service web. *Indication:* Tous les espaces sont remplacés par des underscores (« _ »).
`req-method`	Nom de la méthode du service web qui est appelé dans la requête.
`orig-req`	Point d'origine (URL) sur le proxy service web. *Indication*: Tous les espaces sont remplacés par des underscores (« _ »).
`optional fields`	A l'avenir, différents champs s'ajouteront ici.